



DEPARTMENT OF THE NAVY
NAVAL SUPPLY SYSTEMS COMMAND
5450 CARLISLE PIKE

PO BOX 2050
MECHANICSBURG PA 17055-0791

NAVSUPINST 5530.1D
SUP 03X
28 August 2001

NAVSUP INSTRUCTION 5530.1D

Subj: NAVAL SUPPLY SYSTEMS COMMAND (NAVSUP) SECURITY MANUAL

Encl: (1) NAVSUP Antiterrorism/Force Protection (ATFP)
Security Manual and Plan

1. Purpose. To augment basic guidance provided by references (a) through (av), to establish policy, set uniform standards and provide specific guidance for the execution of additional security measures essential to the unique requirements of field activities of NAVSUP.

2. Cancellation. NAVSUPINST 5530.1C and NAVSUPINST 5530.2A. This regulation is a complete revision and should be read in its entirety.

3. References and Guidance. Appendix A lists references (a) through (av) which are cited in this instruction.

4. Scope. This instruction serves as the basic NAVSUP directive relating to the implementation of the referenced Secretary of the Navy (SECNAV) and the Office of the Chief of Naval Operations (OPNAV) security programs and is to be used in conjunction with references (a) through (av). The provisions apply to all military and civilian personnel at all NAVSUP activities.

5. Discussion. NAVSUP is responsible for providing essential services and supplying materials critical to the Navy to perform its mission which is vital to national security. We have a responsibility to provide employees with a secure environment in which to work. NAVSUP is responsible for physical security and loss prevention efforts for the protection of the materials in the Navy supply system. The personal attention and support of each commander, commanding officer, director or officer in charge is essential to the success of these programs.

6. Policy. This instruction is the basic NAVSUPSYSCOM directive relating to information, personnel, industrial, material, physical security, ATFP and loss prevention programs.

0526-LD-100-8326

NAVSUPINST 5530.1D
28 August 2001

Because of the criticality of these missions, sensitivity of materials and complexity of security programs, NAVSUP activities meeting the requirements of references (a), (d) or (q) will assign a GS-0080 series security director and security manager to manage its security programs. The security director shall be a staff code and have direct access to the commanding officer and executive officer.

An essential element of these programs is the training in loss prevention and security responsibilities and assigning accountability to each person involved in processing material or supply documentation. Security program initiatives shall be based on prudent measures to counter the loss potential.

7. Action. Commanding officers, commanders, directors and officers in charge in the NAVSUP claimancy will ensure compliance with the provisions of this instruction as set forth in enclosure (1) and references (a) through (av) as set forth in Appendix A.



J. D. McCARTHY
Commander

Distribution:

SNDL FKM (Shore activities under the command of NAVSUP)
NAVSUP X(32) (All Offices and Directorates)

Copy to:

NAVSUP 35C (3 copies), 09PAM, 09I, 093, 03X (25 copies)

Order from:

Navy Inventory Control Point
COG "I" Material
700 Robbins Avenue
Philadelphia PA 19111-5098

NAVSUPINST 5530.1D
28 August 2001

NAVAL SUPPLY SYSTEMS COMMAND



SECURITY MANUAL

Enclosure (1)

TABLE OF CONTENTS

<u>CHAPTER</u>	<u>TOPIC</u>	<u>PAGE</u>
Chapter 1	Introduction	1-1
Chapter 2	Personnel Security	2-1
Chapter 3	Information Security	3-1
Chapter 4	Industrial Security	4-1
Chapter 5	Physical Security	5-1
Chapter 6	ATFP	6-1
Chapter 7	Material and Supply Systems Integrity	7-1
Chapter 8	Accounting Procedures for Missing, Lost Stolen or Recovered Material	8-1
Chapter 9	Communications Security Materiel System	9-1
Chapter 10	Security Education Training and Briefings	10-1
Appendix A	References	A-1
Appendix B	Controlled Inventory Items Code	B-1
Appendix C	Criteria for Designating Automated Information Systems (AIS) Position Sensitivity	C-1
Appendix D	Instructions for Completing a DD-254	D-1
Appendix E	Mail Center Security	E-1

CHAPTER I

INTRODUCTION

1. This manual and plan are designed to supplement references (a) through (av) (Appendix A) and make implementation of quality security programs at NAVSUP activities a streamlined and standardized process.

2. Commanding officers are responsible for physical security, loss prevention, ATFP, personnel security and the industrial security program within their commands. The commanding officer shall designate, in writing, both a command security officer and a command security manager. For purpose of clarity, this instruction will use the title Director of Security as an all-encompassing term to include the existing titles and duties of security officers, security directors, directors of security and like titles.

3. The director of security and the security manager are the designated representatives of the command.

a. The director of security must be designated by name and identified to all members of the command on organization charts, telephone listings and rosters.

b. The director of security and the security manager will coordinate appropriate security requirements for their designated functions. Your commands may perform specified security functions for other commands and other commands may provide support to your command. When those conditions exist the director of security will review all partnership agreements, Inter-Service Support Agreements (ISSA), Memorandum of Agreements to ensure security requirements are clearly identified in the partnership agreement.

c. The ISSA may be generic but it will be appended to address specific security requirements. The list must clearly define where the security responsibilities of each participant begin and end. The agreement will include requirements for advising commanding officers of any matters that may directly affect the security posture of the command.

4. Since the Installation Claimant Consolidation (ICC), NAVSUP security requirements have changed. All internal security requirements remain our responsibility at all locations. Host activities remain our responsibility only at certain designated activities. NAVSUP activities providing services to non-NAVSUP activities should assess any added costs to the serviced activity. NAVSUP activities providing recurring services to

NAVSUPINST 5530.1D
28 August 2001

another NAVSUP activity many not charge for those services.

5. Each activity will develop and publish consolidated security instructions relative to the applicable functional program. The security office of the next higher echelon command will review activity security plans.

SECNAVINST 5510.30 Appendix C, SECNAVINST 5510.36 Exhibit 2A and OPNAVINST 5530.14A Chap 2 Para 0201 provide listings of required guidelines that need to be included as part of your local security instruction.

6. Each NAVSUP activity's director of security will complete and forward an annual security report to NAVSUP 03X not later than 1 November that will cover the previous fiscal year. The format for the report will be provided under separate cover. A budget report will be submitted for identifying midyear requirements not later than 14 February. Annual budget input will be provided as directed by NAVSUP 03X. This report provides a synopsis of the activity security program.

7. Information requested relative to overall NAVSUP security program issues will be forwarded via NAVSUP for reporting purposes.

CHAPTER II

PERSONNEL SECURITY

1. This chapter along with the Department of Defense (DOD) Regulation 5200.2-R and SECNAVINST 5510.30A will be used to implement the command personnel security program. Waivers to DOD 5200.2-R and SECNAVINST 5510.36A will be routed via NAVSUPHQ Code 03 to Chief of Naval Operations (CNO) N09N2.

2. The security manager at each NAVSUP activity will serve as the principal control office for administering all functions of the personnel security program. The security manager is the principal advisor on personnel security in the command and is responsible for the management and oversight of the program.

3. Personnel security standards must be applied to determine whether a person is eligible for access to classified information or assignment to sensitive duties. This is based on all available information, the person's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly consistent with the interest of national security.

a. Commanding officers will designate each civilian position in their command as either special sensitive, critical-sensitive, noncritical-sensitive or nonsensitive. Criteria for designating AIS pertaining to position sensitivity are found in Appendix C.

b. All positions should be reviewed periodically to clearly determine the appropriate position sensitivity.

c. In cases where the Personnel Security Appeals Board denies or revokes a clearance or the ability to hold a sensitive position, the employee must either be removed from service or assigned to a nonsensitive position. Positions cannot be redesignated after the command has been notified of an employee's ineligibility for a security clearance.

4. The security manager will ensure clearances are kept to an absolute minimum level. Continuous evaluation of cleared personnel will be conducted to ensure they continue to be trustworthy following the standards in DOD 5200.2-R and SECNAVINST 5510.30A.

5. Supervisors do not review the security forms of anyone undergoing a periodic reinvestigation. Supervisory knowledge of any significant adverse information is to be independent of the information reflected on the security form.

NAVSUPINST 5530.1D
28 August 2001

6. The security manager will ensure initial and refresher briefings to individuals with security clearance eligibility are conducted. These briefings will emphasize the individual's responsibility to meet the standards and criteria for a security clearance as stated in DOD 5200.2-R and SECNAVINST 5510.30A.

7. Individuals possessing a security clearance will report to their security manager or supervisor contacts with individuals of any nationality whether within or outside the scope of the employee's official activities, when:

a. Illegal or unauthorized access is sought to classified or otherwise sensitive information.

b. Individuals are concerned they may be the target of exploitation by a foreign entity.

8. OPNAV Form 5510/413, Personnel Security Action Request, will not be submitted for the following:

a. When an individual transfers from your command.

b. When an individual's level of access has been downgraded unless there is a permanent change in official duties (i.e., rating/measure of stability) eliminating the requirement for a security clearance/access.

9. Do not send in duplicate copies or tracers of the OPNAV Form 5510/413 until you have waited 270 days from the date of the original correspondence. The Department of the Navy (DON) Central Adjudication Facility (CAF) will not take action.

10. When sending OPNAV Form 5510/413 requests or any correspondence to the DON CAF, please include your e-mail address along with a commercial and DSN phone number and point of contact.

You are no longer required to request a clearance from the DON CAF when a new member arrives at your command. You may grant access as long as you have a DON CAF security clearance certification message in the member's personnel file and:

a. The individual continues compliance with the security standards;

b. The individual has had no subsequent break in service exceeding 24 months since the date of the certification message; and

c. Access does not exceed the level approved on the DON CAF certification message.

11. Temporary access may be granted to DON personnel who have been otherwise determined to be eligible for a security clearance by the DON CAF but do not currently require a security clearance/access to perform assigned duties.

12. Security managers must maintain a record of all accesses granted including temporary accesses, special accesses or other program accesses such as North Atlantic Treaty Organization Secret, Critical Nuclear Weapon Design Information, Sensitive Compartmented Information (SCI) and Personnel Reliability Program. The following information must be recorded:

- a. Name,
- b. Social Security Number,
- c. Citizenship verification,
- d. Date and level of access authorized,
- e. Basis for access determination, and
- f. Name, title, rank/grade of authorizing individual.

13. If no record of a previously signed Classified Information Nondisclosure Agreement (Standard Form (SF)-312), all DON military and civilian personnel must sign the current version of the SF-312 before being given access.

14. Remember, only security managers and other authorized security personnel can contact the DON CAF on security clearance issues.

15. Defense Clearance and Investigations Index checks will be provided by NAVSUPHQ on request.

16. Individuals granted initial top-secret security clearance and/or initial indoctrination into a Special Access Program (SAP) or to SCI will orally attest to understanding their responsibility to protect classified national security information. Commands will document the completion of this one-time attestation. Exhibit II-1 provides the documentation required for the attestation.

NAVSUPINST 5530.1D
28 August 2001

EXHIBIT II-1

PERSONAL ATTESTATION
UPON THE GRANTING OF A
SECURITY CLEARANCE AND/OR ACCESS TO
TOP SECRET AND/OR SCI OR SAP

Ref: (a) OASD (C3I) ltr of 09 Feb 99
(b) SECDEF ltr of 05 Feb 99
(c) CNO msg 092137Z of Apr 99

I _____ ATTEST TO THE
FOLLOWING: (Print name)

"I ACCEPT THE RESPONSIBILITIES ASSOCIATED WITH BEING GRANTED ACCESS TO CLASSIFIED NATIONAL SECURITY INFORMATION. I AM AWARE OF MY OBLIGATION TO PROTECT CLASSIFIED NATIONAL SECURITY INFORMATION THROUGH PROPER SAFEGUARDING AND LIMITING ACCESS TO INDIVIDUALS WITH THE PROPER SECURITY CLEARANCE AND/OR ACCESS AND OFFICIAL NEED TO KNOW. I FURTHER UNDERSTAND THAT, IN BEING GRANTED ACCESS TO CLASSIFIED INFORMATION AND/OR SCI, SAP, A SPECIAL CONFIDENCE AND TRUST HAS BEEN PLACED IN ME BY THE UNITED STATES GOVERNMENT."

ATTESTED BY:

WITNESSED BY:

Signature & Date

Signature & Date

BRIEFED BY:

Signature & Date

CHAPTER III

INFORMATION SECURITY

1. Protecting information is critical to mission accomplishment. The goal of the Information Security Program is to efficiently and effectively protect information by delegating authority to the lowest levels possible; encouraging and advocating use of risk management principles; focusing on identifying and protecting information that requires protection; integrating security procedures so they become transparent; and, ensuring everyone understands their security roles and responsibilities and *takes them seriously*.

2. The security manager is the principal advisor on information security in the command and is responsible to the commanding officer for the management of the program. The security manager at each NAVSUP activity shall serve as the principal office for oversight on all functions of the Information Security Program.

3. Waivers of classified material handling and storage procedures will be strictly monitored. All countermeasures listed in the waiver/exception must be completed. If the countermeasures are not implemented it may result in an Inspector General finding.

4. Each command is responsible for ensuring their emergency plans include procedures for the Secure Telephone Unit-Third Generation (STU III) telephones.

5. Training is the key to an effective information security program. Commanding officers are responsible for ensuring security personnel are adequately trained to perform their duties whether full-time or part-time. The security manager is responsible for ensuring annual refresher briefings are conducted. The security manager will ensure the following training is conducted relative to information security.

a. Meetings are scheduled and conducted with custodians of classified material at least annually. This provides an opportunity to discuss new procedures, problem areas and resolve questions.

b. In addition to normal basic security indoctrination, employees who are designated as the classified material custodians (classified documents and equipment) will be given specialized training to cover the following subjects:

- (1) Security classification categories and markings;
- (2) Command control system including receipts,

NAVSUPINST 5530.1D
28 August 2001

recording, routing, reproducing, transmittal, retirement and destruction;

(3) Access requirements;

(4) Storage requirements; and

(5) Safeguarding requirements, including protection of combinations to locking devices.

(6) The training material will include specific procedures; i.e., desk guides, local instruction, etc., which the employee will retain for daily reference. Copies of desk guides and local instructions will be provided to custodians by the security manager's office.

c. Personnel handling classified contracts will receive specialized training in security requirements outlined in DOD 5220.22M and 5220.22R.

6. Administrative procedures will be established to account for secret material other than messages. At a minimum, the control system will provide for a central point of control for classified material and a control register for incoming and outgoing classified. A receipt is required when transmitting secret material. While secret messages need not be entered into the control system, they should be carefully monitored to ensure proper storage and destruction.

7. Classified secret messages should not be held in storage over 30 days. If a requirement exists to maintain the messages beyond the 30-day period, they will be properly logged in and accounted for under the established control procedures.

8. Signing the Nondisclosure Agreement (NDA) is a prerequisite for obtaining access to classified information or material. No access will be granted without ensuring the employee has signed the NDA.

9. Each activity will ensure the end-of-day security checks are conducted to ensure classified material is stored appropriately. Personnel conducting these checks will do so at the close of each working day and record them on the Activity Security Checklist (SF-701), and the Security Container Check Sheet (SF-702), when security containers are present.

10. Security managers will develop security procedures that ensure control of reproduction of classified material. For copiers and facsimile machines or any machines with copying capability (i.e., microfiche machines), the information security manager will coordinate with their servicing agency to determine

if the machines are authorized for copying classified. They will identify if they retain any latent images when copying classified and what procedures are necessary to clear them when they process classified.

When they need to be cleared, destroy the waste as classified material when latent images are visible. Machine custodians must post a notice on machines approved for copying classified to inform users of the authority and clearance procedures.

11. Debriefing all individuals with security clearance eligibility is required when they terminate civilian employment, separate from the military service, have their access suspended or terminated or have their clearance revoked or denied.

12. The security manager will be responsible for ensuring inventories of top secret holdings are scheduled at least annually. A report will be maintained in the security office of the results of the inventories.

13. Original classification is involved when an item of new information is developed which requires classification in the interest of national security and when such classification cannot reasonably be derived from or closely related to similar information. NAVSUP does not have original classification authority. NAVSUP creates classified information from derivative classification that is accomplished by incorporating, paraphrasing, restating information that is already classified. This can be determined by consulting the classification guides available for review from the security managers.

14. If classified meetings are to be conducted, the security manager must be notified. Proper procedures for conducting classified meetings must be in conjunction with reference (e).

15. An annual clean-out day for classified information will be conducted at each activity.

16. Security at mail center facilities will be in compliance with Appendix E and where applicable (references (aq), (ar) and (as)).

a. Inspection of the mail center will include the handling, storage and accounting of classified material.

b. Security containers are required for storing both classified and registered mail.

c. Combinations of containers used to store registered mail and classified mail will be changed annually when there is a

NAVSUPINST 5530.1D
28 August 2001

change of mail clerks, and when an actual or suspected compromise occurs.

d. Maintenance and operation of the STU III will be provided to ensure proper operation and storage of classified material.

17. All non-General Services Administration (GSA) approved containers will be replaced with GSA-approved containers as soon as feasible prior to the mandatory replacement date of 1 October 2002.

CHAPTER IV

INDUSTRIAL SECURITY

1. The Contracting Officers Security Representative (COSR) shall be designated in writing. The COSR designation shall be for the purpose of signing the Contract Security Classification Specification (Department of Defense (DD) Form 254), and revisions thereto. The COSR will be a knowledgeable security representative. The COSR is responsible to the security manager for coordinating with program managers and procurement officials. The COSR shall ensure the industrial security functions specified in Chapter 11 of reference (d) are accomplished when classified information is provided to industry for performance on a classified contract.

2. The following industrial security responsibilities are normally assigned to the COSR but are not limited to the following:

a. Review statement of work to ensure access to or receipt and generation of classified information is required for contract performance.

b. Validate security classification guidance, complete and sign the DD-254:

(1) Coordinate review of the DD-254 and classification guidance.

(2) Issue a revised DD-254 and other guidance as necessary.

(3) Resolve problems related to classified information provided to the contractor.

c. Provide when necessary, in coordination with the program manager, additional security requirements beyond those required by this regulation in the DD-254 or the contract document itself.

d. Initiate all requests for Facility Security Clearance (FCL) action with the Defense Security System (DSS) Operations Control Center.

e. Verify the FCL and storage capability prior to release of classified information.

f. Validate justification for interim top secret Personnel Clearances and FCLs.

NAVSUPINST 5530.1D
28 August 2001

g. Validate and endorse requests submitted by industry for Limited Access Authorizations for non-U.S. citizen employees of a cleared contractor.

h. Coordinate, in conjunction with the appropriate transportation element, a suitable method of classified shipment when required.

i. Review requests by cleared contractor for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions or issue a final DD-254.

j. Certify and approve Registration for Scientific and Technical Information Services Requests (DD-1540).

k. Review reports of security violations and compromises within industry and forward to program managers.

l. Ensure timely notice of contract award is given to host commands when contractor performance is required at other locations.

3. Commanding officers shall ensure a Contract Security Classification Specification (DD-254) is incorporated into each classified contract. An original DD-254 shall be issued with each request for proposal, other solicitations, contract award, or follow-on contract to ensure the prospective contractor is aware of the security requirements and can plan accordingly. A revised DD-254 shall be issued as necessary during the lifetime of the contract when security requirements change. A final DD-254 shall be issued on final delivery or on termination of a classified contract. Training will be provided to all contracting officers who service classified contracts. A guide for the preparation of a DD-254 is provided in Appendix E.

4. The Internal Security Act of 1950 entrusts commanding officers to protect persons and property against the actions of untrustworthy persons. Within DON the Facility Access Determination (FAD) Program assists commands in making trustworthiness determinations on contractor employees for access eligibility to controlled unclassified information or sensitive areas and equipment under DON control. Trustworthiness determination pertains to unclassified contracts for various services (e.g., janitorial, guard, equipment maintenance). Commands shall take the necessary steps to include the conditions of the FAD Program in the specifications of all contracts needing trustworthiness determinations, thereby eliminating the necessity to award a classified contract for performing services only. Reference (d) addresses specific requirements for administering the FAD Program.

5. Many NAVSUP activities have contracts requiring contractor access to NAVSUP information systems, nonsensitive unclassified information or areas critical to the operations of the command. These contracts are not classified and therefore contractor employees are not required to obtain a National Agency Check (NAC). However, a facility access determination is required. Reference (a) states "Commands will include FAD program requirements in the contract specifications when trustworthiness determinations will be required on the contractor employees."

6. Reference (a) states that a contractor whose work involves access to sensitive unclassified information warrants a judgment of an employee's trustworthiness. Therefore, all personnel accessing NAVSUP computer systems must undergo a FAD NAC to verify their trustworthiness.

7. In order to comply with these requirements the following text is required to be in all NAVSUP contracts or solicitations where the contractor has access to computer systems or other business information systems:

Trustworthiness Security Text

"Each contractor employee will have a favorably completed NAC. If contractor personnel currently have a favorably adjudicated NAC, the contractor will notify the security manager of the command they will visit by providing the information relative to the investigating agency, the type of investigation and the date. The visit request will be renewed annually or for the duration of the contract if less than 1 year."

If the contractor employee is a foreign national, prior approval of the Network Security Officer is required. Access may be granted to foreign nationals who have a need to know and at least one of the following applies:

- a. Foreign national is employed by DOD, or
- b. Foreign national possesses a current functional accreditation approved by the Navy International Program Office, or
- c. Foreign national possesses a current Visit Request Form (OPNAV 5521/27 Rev 1-73) (as defined in SECNAVINST 5510.36) which provides the investigative information, and it is on file with the requesting activity.

8. If no previous investigation exists, contractor personnel will complete the requirement for trustworthiness NAC. The

NAVSUPINST 5530.1D
28 August 2001

trustworthiness NAC is processed through the command security manager. The NAC will be processed through the use of the Electronic Personnel Security Questionnaire (EPSQ) (SF-85P). The EPSQ software can be downloaded at the DSS website <http://www.dss.mil/epsq/index.htm>.

The contractor should provide the completed EPSQ electronically (electronic mail/diskette) to the command security manager along with the original signed release statements and two applicant fingerprint cards (Federal Document 258). The responsibility for providing the fingerprint cards rests with the contractor. The security manager will review the form for completeness, accuracy and suitability issues. The completed SF-85P along with attachments will be forwarded to Office of Personnel Management who will conduct either the trustworthiness NAC or NAC.

9. The DON CAF will provide the completed investigation to the requesting command security manager for the trustworthiness determination. The command will provide written notification to the contractor advising whether or not the contractor employee will be admitted to command areas or be provided access to unclassified but sensitive business information.

10. Contractor employees are not Government employees. They are governed by the terms of the contract and they are not covered by local instructions. Contractor's use of Government resources can blur the distinction between the Government and the private sector. All individuals we make contact with must know whom they are dealing with. By clearly identifying contractor personnel it provides the general public, other DON activities, and our own workers the ability to know with whom they are dealing and it therefore avoids inadvertent disclosure of nonpublic information.

The following measures will be established to clearly identify all NAVSUP contractor employees.

a. Distinctive security badges. The badge will be provided to coincide with the contract or up to 1 year, but no longer than 1 year.

b. The ideal solution is to locate all contractor personnel in one clearly identified work area. However, when that is not possible, clearly identify the office space occupied by contractor personnel.

c. Contractors who are provided access to an e-mail address will be clearly identified as contract employees. Foreign contract personnel will not only be identified as a contractor but also as a foreign national.

CHAPTER V

PHYSICAL SECURITY PROGRAM

1. Security Planning

a. Each NAVSUP activity will develop and publish a physical security and loss prevention plan in consonance with regional commanders and their security coordinators and their senior command that complies with reference (q).

b. Internal security plans for NAVSUP activities that are tenant activities on a Navy installation will be integrated into the installation physical security plan as appropriate. The plan will incorporate requirements, policies and procedures for facilities, equipment, regular and auxiliary security forces, employee training/education and other elements of security essential to force protection and objectives set forth by reference (q).

2. Command Physical Security Review and Assessment

a. The commanding officer of a Navy activity is expected to establish a continuing program of systematic physical security review and assessment. Every activity must review its local processes in conjunction with host installations and other activities in the region to come up with ways of providing physical security that meets standards in an efficient manner that is affordable.

b. In addition, appropriate local participation in such a program of physical security review and assessment is detailed in reference (q). A record of the review meetings will be maintained.

3. Physical Security Surveys

a. OPNAVINST 5530.14C requires an in-house assessment of an activity's physical security program including loss prevention and ATPF. It includes a complete study and analysis of each activity's property and operation, as well as physical security measures in effect.

b. In terms of our NAVSUP activities, with the exception of Naval Inventory Control Point Mechanicsburg (NAVICP-M) being a host activity security provider, the in-house assessment should be in participation with your regional assessment.

c. An assessment synopsis, including deficiency corrective options, will be provided to NAVSUP in order to prepare, prioritize, support and budget for security budget submissions.

NAVSUPINST 5530.1D
28 August 2001

This should be submitted to NAVSUP Code 03XA by 14 February of each year in order to plan for funding requirements.

d. NAVICP-M will comply as a host activity security provider.

e. The results of physical security surveys are key to the activity/installation/regional physical security and loss prevention review and assessment programs. Accordingly, the surveys need to be kept updated so these review and assessment processes are based on current, complete and accurate data.

4. Vulnerability Assessments

a. As described in OPNAVINST 5530.14C, NAVSUP will conduct vulnerability assessments using CNO (N34) vulnerability assessment checklist every 3 years for all activities with the exception of the NAVICP, which falls within the 'over 300 category' requirements.

b. Copies of any assessments conducted by CNO (N34) or Joint Staff/Defense Threat Reduction Agency teams will be furnished to NAVSUP.

5. Threat Assessments

a. Security programs cannot be restricted to protection of most critical assets and facilities, but must be a continuous program to protect all assets and facilities and capable of minimizing daily threats and expanding to encompass increased threat conditions.

- Theft (both systematic and casual)
- Bomb Threats
- Workplace Violence
- Natural Disasters
- Sabotage
- Terrorism
- Subversion
- Hostage/Barricade Situations

b. In addition to requirements of reference (q), internal threat condition procedures shall be established following requirements and guidelines outlined in reference (ai) and included in the applicable security plan.

6. Activity Upgrade Requirements/Waivers/Exceptions

All activities will review their existing security posture due to organization and functional support changes, due to the ICC to determine modifications necessary to conform to reference (q).

Any internal waivers/exceptions required will be submitted to NAVSUP 03 per reference (q). They will be consolidated as a NAVSUP-wide waiver or exception when they are identified. External waivers/exception involving regional security issues should be coordinated with the region and NAVSUP 03.

7. Restricted Areas. Appendix VI to reference (q) gives policy for the three levels of restricted areas and the minimum-security measures appropriate for those levels. Due to the Navy ICC changes and the establishment of the Navy regions, NAVSUP activities need to review their restricted areas and ensure they comply with reference (q).

8. Key Security and Lock Control

a. Each activity must have a key and lock control program for all keys, locks, padlocks and locking devices used to meet security and loss prevention objectives of reference (q).

b. It is not intended to include keys, locks and padlocks used for convenience, privacy, administrative or personal use. The security key and lock control procedures and inventories shall be only for security and loss prevention objectives of reference (q).

9. Protection of Bulk Petroleum Products. Guidelines for the protection of bulk petroleum products will conform to reference (q). Guidelines pertain to Government-owned, Government-operated and Government-owned, contractor-operated fuel support points, pipeline pumping stations and piers.

10. Access Control. OPNAVINST 5530.14C defines access control for installation and tenant activities. Internally, NAVSUP activities designate restricted areas and access controls in security planning.

11. Property Passes

a. The Optional Form (OF) 7 will be used at all NAVSUP activities vice the previously used NAVSUP Form 155. The form is prescribed by GSA and should be accepted by other than NAVSUP activities as prescribed by the Federal Property Management Regulations 41 CFR 101-20.110.

b. Existing security procedures requiring a property pass should be reviewed and revised to include the OF-7.

c. The OF-7 can be obtained through the GSA system, National Stock Number (NSN) 7540-00-634-4264.

NAVSUPINST 5530.1D
28 August 2001

d. A listing of personnel authorized to sign property passes should be provided to the security office. A Signature Card (DOD Form 577) will be prepared for each individual authorized to sign property passes. Where required, gates and other authorized exit points will have a current listing of personnel authorized to sign.

e. Material from storage sites may be removed on supply documentation.

12. Found Property Procedures

a. This establishes and formalizes procedures to be followed when personal currency or property is reported as lost or found at NAVSUP activities. Unclaimed property will not be used to generate funds for any organization, regardless of the worthiness of the cause. Substantial sums of money, if not claimed, will be remitted to the U.S. Treasury, normally within 72 hours. The field office security director is designated as the responsible officer for administering the lost and found process. Those responsibilities include security of the items, maintenance of records and actions taken to return the property to the rightful owner or other disposition.

b. When found, property exceeding \$100.00 in value or when any money is surrendered to the security office, the following procedures will be adhered to:

(1) The security office representative will immediately complete a Found Property Tag (GSA Form 252). When appropriate, the lower part of the form will be given to the person surrendering the property. The upper part of the form will be attached to the item.

(2) A Record of Property Found/Attempts to Contact Owner of Found Property (GSA Form 1039) will be maintained at each found property facility. The form will be maintained until all property listed thereon has been transferred to storage, disposed of or released to owner. Completed forms will be retained for 2 years.

(3) Found property custodians will be appointed in writing. A list of authorized custodians will be posted to each container where found property is stored and only those personnel or the security director will be allowed admittance. Property custodians will be responsible for listing each item of property on the GSA Form 1039 maintained at the storage facility and making it available for inquiries.

The property custodian is responsible for security and disposition of all property stored at the facility. Attempts to contact owners will be recorded the back of the GSA Form 1039.

(4) Safeguarding found property is the responsibility of the custodian. Found property will be stored in a filing cabinet or safe with a built-in combination. A filing cabinet will be equipped with a locking bar and at least a medium security padlock.

(5) When the owner of found property is identified, the custodian will notify the owner by certified mail the property is in custody and the scheduled disposal date. The return receipt from the certified mail will be attached to the GSA Form 252. If the property is not claimed within 60 days of the certified letter, it will be disposed of.

(6) Property will be held no less than 60 days, except contraband, which will be disposed of following local directives. Appropriate turn-in documentation will be prepared by the custodian for property to be turned in to Defense Reutilization Marketing Office (DRMO) (normally DD Form 1348-1A). When turn-in is complete, the GSA Form 1039 will be annotated with date and method of disposal. Currency will be turned in to the dispersing officer and a receipt obtained. In the event the owner of currency is identified, the custodian will forward the name and address of the owner to the dispersing officer.

(7) Inventory of found property will be conducted by a disinterested third party designated by the field office security director. Inventories will be conducted quarterly and recorded on the GSA Form 1039. When found property is determined to be missing, it will be reported to investigative authorities.

(8) If the command has access to the electronic forms database, forms may be accessed electronically. Otherwise all relevant forms may be obtained from the National Forms and Publications Center, 4900 S. Hemphill Street, Warehouse #4, Dock #1, Fort Worth, Texas 76115.

13. Identification Badge Standards

a. Reference (q) requires a system of personnel and vehicle identification at all naval installations and activities. In NAVSUP, the Navy Electronic Badging System (EBACS) will be the standard for identification of personnel and control of visitors. The EBACS badge is the preferred badge for access to NAVSUP commands and activities and as installation identification.

Visitors from other NAVSUP activities should be authorized access based on their possession of a valid EBACS-issued badge. EBACS badges will be issued for a period not to exceed 6 years. Lost badges will be reported to the issuing security office immediately.

NAVSUPINST 5530.1D
28 August 2001

b. Contractor badges should be clearly identifiable by color to distinguish them from NAVSUP employees, even if issued by other than the NAVSUP activity. Badges should not exceed 1 year or the duration of the contract, whichever ever comes first.

c. U.S. Government Identification (OF-55). NAVSUP endorses and supports the continued issuance of the OF-55. Currently it is the only civilian employee badge universally recognized. The OF-55 is available through GSA. It is the only identification that is accepted throughout DOD and for employees who have a need to travel overseas, to other service installations and even within DON installations, activities and ships. The following guidance is provided:

(1) Where feasible, local NAVSUP activities will coordinate issuance with their servicing badging office.

(2) If practical, NAVSUP activities will procure and retain the form, sending employees to their servicing badging office with a blank form when a card is needed.

(3) Maintain a log identifying the employee it was issued to. Include other relevant information found on the card to assure accountability.

(4) Establish lost badge procedures.

(5) Establish recovery of the badge when it expires, the employee transfers or retires.

(6) The OF-55 will not be issued to contractor or military personnel.

(7) Duration of issue will be left to the discretion of the director of security; however, consideration will be given to shorten expiration dates if warranted.

d. Identification badges will be worn at all times. The badge will be visible, above the waist with the photograph facing out. The badges will not be defaced by sticking pins or other items through the badge. Many badges contain embedded items that can be damaged when items are inserted through the badge.

14. Security of Mail. Many NAVSUP activity security offices have been tasked with the security of mail functions. Guidelines and policy for those functions are contained at Appendix E.

15. Organizational Relationships

a. Since the Navy ICC has occurred, there have been many

changes in organizational relationships and support. We must continue to identify how our relationships with host commands and tenants have affected our external and internal security posture. There must be a close relationship of host/tenant physical security review and assessment. Specific goals include identification of employment of specific physical security measures that efficiently meet all the security interests and needs of individual activities and installation (host/tenant) in a manner that avoids waste of resources.

b. Guidelines for installation and regional (host) security review and assessment are contained in reference (q).

16. The Security Force

a. Navy military, civilian and contract personnel regularly engaged in law enforcement or security guard duties shall be armed.

(1) No person will be armed unless currently qualified in the use of assigned weapons. In order to qualify, Navy military and civilian personnel performing law enforcement or security guard functions must satisfactorily complete the firearms training outlined in reference (aa).

(2) No contract guard will bear firearms onboard a Navy installation or activity until written certification of qualification meeting Navy standards (reference (m) pertains)) is provided by the contractor, and the guard has successfully completed training in the use of force and rules of engagement. In addition, contractors must comply with provisions prescribed by the state in which the contract is administered, including licensing and permit requirements.

b. Mandatory requirements and guidance concerning use of force including deadly force are outlined in reference (z).

CHAPTER VI

ATFP

1. Terrorist and criminal attacks on U.S. Government personnel have claimed the lives of over 300 persons in the last 20 years. At least 600 persons have been injured in the same period. No U.S. Government affiliated persons are immune from the risk of terrorist or criminal attack. Officers, enlisted and civilian employees have all been victims. Even persons in the continental U.S. are not immune to terrorists. Individual awareness and training are essential elements of the force protection program. Knowledge of self-protection measures is a means to deter and lessen the impact of terrorist attacks. The protection of DOD personnel and assets is a complex command challenge. It is the inherent responsibility of the command to protect personnel. Planning to confront this challenge requires a comprehensive, integrated approach per references (j) through (q). Careful preparation is the focus of the ATFP Program.

2. The DOD combating terrorism program stresses deterrence of terrorist incidents through preventive measures. The program addresses:

- a. Threat analysis.
- b. Integrated criticality and vulnerability assessments.
- c. Threat assessment based on the threat analysis friendly vulnerabilities.
- d. Operations, personal, industrial and physical security.
- e. Crisis management planning.
- f. Continuous training and education of personnel.
- g. Limited response and containment.

3. The ATFP Program seeks to reduce the likelihood that DOD affiliated personnel, facilities and material will be attacked and to mitigate the effects of such attacks should they occur. The program has two phases. There is a preventative phase in which the threat is identified; assess risk, vulnerability and criticality of installations, personnel and material; promote awareness and conduct education and training of personnel in preventive measures; and develop plans and programs to prevent, respond, contain and resolve terrorist incidents should they occur. There is also a reactive phase in which crisis management plans are implemented and terrorist incidents resolved.

NAVSUPINST 5530.1D
28 August 2001

4. All shore installations and bases are required to designate Force Protection Officers (FPO). Graduates of the ATFP responsible officer course will perform FPO duties and will conduct Level I antiterrorism training. Therefore, each applicable activity will have an individual certified to conduct ATFP training per references (n) through (q). Training consists of a program of instruction delivered by a certified instructor which includes personal awareness videos and receiving two documents: Joint Staff Guide 5260, "Service Member's Personal Protection Guide, a Self-help Handbook to Combating Terrorism," and "Antiterrorism Individual Protective Measures" folding card. This training also must include a current briefing on the threat for the area of travel. Threat assessments, classified or unclassified, will be provided covering the specific area of travel. Training will be completed prior to travel.

5. By their nature, security duties are involved with counter-terrorism activities. While the director of security may not have the police/guard forces to directly confront a terrorist operation, he/she must be involved in advance planning to deal with such a contingency. NAVSUP activity security operations should maintain close liaison with local Naval Criminal Investigative Service (NCIS) personnel as well as regional and local law enforcement departments in addressing threats and counteractions. The protective measures for each threat condition must be considered. Those that are applicable to a NAVSUP activity must be expanded, localized and published in the Physical Security and Loss Prevention Plan.

6. Reference (k) identifies mandatory standards to implement the antiterrorism portion of the broad DOD force protection program. Appendix C of reference (k) contains a Physical Security Survey Instrument that can be utilized as part of the command review.

CHAPTER VII

MATERIAL AND SUPPLY SYSTEMS INTEGRITY

1. The purpose of this chapter is to establish policy to ensure identification and accountability of Navy material throughout its lifecycle, regardless of its location.

a. Pertinent references are contained in Appendix A. The provisions of this section are applicable to all DON activities that provide inventory management, store, stage or transport U.S. Government material, as well as those that take custody for end use. References (al) through (ap) form the basis of this directive and may be referred to for expansion of the precepts outlined herein.

b. Appendix B is a listing of controlled inventory items including security, pilferage codes and other supply codes encoded in the various records and material movement documents. Knowledge of these codes is critical to the security and proper processing of classified, pilferable and sensitive material.

2. Naval and industrial activities hold or process well over \$30 billion of U.S. Government material. Much of this material is vulnerable to theft and misuse by individuals, private enterprise, the criminal element and foreign governments. Much of this material is easily converted to personal use, of high dollar value, not readily available elsewhere, a danger to the public or a danger to the national defense. Accurate accountability of this material is an enormous undertaking and demands conscientious efforts and stewardship. This effort extends through the supply pipeline to the user.

a. In the past, attempts have been made to defeat or abuse the supply system through outright theft or through systematic and more sophisticated manipulation. While theft, both by insiders and burglars, is always a high threat and is the reason to accentuate the importance of physical security programs and measures, system manipulation and collusion are less conspicuous and more difficult to detect. System manipulation does not necessarily mean a person walks out the gate with Government property. Usually system manipulation losses are for greater amounts or of a more sensitive nature; e.g., classified material, difficult to obtain aircraft parts, arms, ammunition and explosives. There is a real concern for requisitioned material being addressed to illegitimate addressees; material signed for but never received by consignee; requisition canceled after material is picked without item manager or customer authorization; insufficient demilitarization records or premature disposal of A-condition parts; and unauthorized access to automated systems and the amount of information available to system users.

NAVSUPINST 5530.1D
28 August 2001

b. Analysis has revealed some inherent sponsor system problems that require command attention to reduce or eliminate material vulnerability. Failure to report improper shipment of material, shortages and losses makes the system appear adequate but does not allow for the targeting of areas with the magnitude of problems and, consequently, does not allow for corrective actions. Partnership sites need to be fully evaluated to ensure material is being properly received and stored and is in compliance with physical security requirements that ensure proper accountability and storage.

c. Increased awareness of the material and system vulnerabilities can be accomplished by enjoining Navy personnel, military, civilian and associated contractors, to serve as vanguards to its integrity and accuracy. Effective use of the supply system depends on proper training of all users, an integral knowledge of the material and accurate coding of the records and material movement documents. Often times the information used to encode the documents, i.e., protect the material, comes from technicians, particularly with regard to repairable parts.

3. Reliability of the supply system coding and procedures is essential to achieve the intent of this directive and to attain the vigilance of Navy personnel. Missing and improper coding has jeopardized the security and accountability of material in the supply system. Reviewing databases with the parameters of the coding contained in Appendix C, and by applying local interpretation of high dollar value items, will enable each activity to focus on special needs/areas to concentrate extra measures.

a. Hardware Systems Commands (HSCs). Planning for systems and inventory accuracy begins with the integrated logistics support plan. Integrated logistics support management teams perform meticulous analysis, detailing and coordination of acquisition projects. HSCs are the inventory managers of the principal item. To enhance the effectiveness of the integrated support, HSCs must perform the following functions:

(1) Identify security and demil requirements in the logistics support analysis record as specified in the Military-Standard.

(2) Consider changes in security and demil requirements in parts and system modification.

(3) Determine declassification and disposal requirements in the logistic support analysis process and incorporate requirements in associated classification guide (usually an OPNAVINST 5513. -- series instruction)

b. NAVSUP. In concert with NAVICP, develop a matrix of special commodity items by authorized or legitimate requisitioners to assist in validating users of critical and/or sensitive items. Develop a requisition lockout procedure that will preclude unauthorized users from procuring specified items.

c. NAVICP/Fleet Material Support Office (FMSO). Through coordination with appropriate Navy activities, will assure accurate security, pilferage, hazardous material and demilitarization codes are recorded in master stock records. It is essential any procurement action include specifications to incorporate necessary coding and handling procedures.

(1) FMSO will ensure material security concerns are incorporated in any computer program package and subsequent modification. Of specific concern is the change notice card procedure whereby changing one field may inadvertently affect other fields whether system generated or a local activity change.

(2) Where applicable, FMSO will incorporate the requirements of this instruction into the Uniform Inventory Control Point, Uniform Automated Data Processing System - Stock Points and Uniform Automated Data Processing System Level II systems.

d. Fleet and Industrial Supply Centers (FISCs) will perform the following actions:

(1) Review storage, security, Master Stock Item Record (MSIR) accuracy and supply-processing procedures for material with codes contained in Appendix B.

(2) Monitor issues to assure only authorized requisitioners, as provided by the NAVICP, are receiving sensitive material. It is important to scrutinize the "ship to" and "bill to" entries on the requisitions to assure a valid requisition is not corrupted. FISCs will develop local programs to scan the requisition status file and count all requisitions within a specified data range. These records are to be compared against the MSIR and if they meet the criteria as a sensitive item, they are to be printed on a report, tailored by the unit identification code which is sent to the customer for their review.

(3) It is strongly recommended the inventory accuracy officer be the focal point to ensure all divisions within the FISC work together to provide proper MSIR line item coding. The importance of controlling these highly sensitive items and ensuring proper action is taken to update the MSIR, and notify the NAVICP of action required to correct line item coding throughout the supply system, cannot be overstated.

NAVSUPINST 5530.1D
28 August 2001

(4) Assist in preventing unauthorized requisitions from being accepted in automated supply systems and establish after-the-fact checks to identify these unauthorized requisitions.

(5) Warehouses and staging areas approved for classified material are also approved for storage and staging of W, 9 and O coded items. All storage areas are considered restricted areas requiring certain protection levels. Provisions for securing and controlling access to a restricted area must be rigorously enforced. It is recognized some storage requirements for other sensitive material, e.g., weapons and precious metal, may be even more stringent.

(6) All transfers of classified material will be accomplished under signature. The instrument for effecting signature control in the transportation system is DD Form 1907 or Air Force (AF) Form 127 for surface movement and AC-10 for commercial air shipments; however, other means, including electronic signature for confidential material, may be available and prescribed between local activities.

(7) Notwithstanding the requirements for signature service for classified material, small arms, R, Q, O, and 9 coded material, shipments of repairable and W codes will be made via traceable means between activities, including local deliveries. Also traceable means should be established for internal transfers of material throughout the warehouse.

(8) Restrict the issue of security code W line items to only authorized users as approved by NAVSUP or cognizant NAVICP.

e. End Use Activities

(1) Procure only those items necessary to perform command mission and only in the quantity needed. Supply officers must be cognizant of the potential of submitting a requisition for a part and having it sent to another activity/address by inserting an entry in card column 45-50 (supplementary address) and card column 51 (signal code).

(2) Ensure personnel are trained in proper material processing in terms of documentation, receipt, stow, issuing, shipping processes and Missing, Lost, Stolen or Recovered (MLSR) reporting requirements.

(3) Immediately report losses, shortages and non-receipt of material by means of a Report of Discrepancy (SF-364) or a Transportation Discrepancy Report (SF-361), as appropriate. Perform survey of lost or stolen material and submit as an MLSR report as prescribed by reference (a1). Conduct quarterly

reviews of MLSR reports and other reports of audits and incidents to detect trends and weaknesses in security, accountability and loss prevention.

(4) Ensure material storage areas are designated and secured as restricted areas.

(5) Ensure technicians and authorized personnel involved in receipt and turn-in of repairable items are familiar with supply, accountability and security aspects of the system.

(6) Ship or deliver classified under signature service or traceable means, as appropriate. Classified receipts and shipments will be accomplished under signature irrespective of the dollar value. **Do not send classified material to the Advanced Traceability and Control Hub.**

(7) **Do not** commingle sensitive material; i.e., classified and unclassified, repairable and general material, in shipping containers.

CHAPTER VIII

ACCOUNTING PROCEDURES MLSR

1. This chapter highlights revised procedures in dealing with classified and sensitive material reporting requirements.
2. Accurate accountability of Government property is necessary and driven by a number of policy documents. Strict accountability for Arms, Ammunition, and Explosives (AA&E) by all agencies within DOD is mandated by reference (y). Reference (r) requires physical security measures for all Government property and the analysis of loss rates through inventories, reports of survey, and criminal incident reports to determine whether losses result from criminal acts or negligent management.
3. A properly run program can help identify losses and loss trends that may go unnoticed through other material management programs. The program requires the cooperation of both the supply and security departments. Both departments must work together to identify material control problems. Although each individual report should be reviewed for possible security weaknesses or impropriety, it is the "trend" of the reports that should provide the most convincing data for resource commitment.
4. Efficient management of Navy resources is a matter of high priority and requires effective loss prevention and physical security programs. Each person is charged with safeguarding Government property under his or her jurisdiction. Property issued to individuals does not become private property by act of issuance or possession, but remains public property, which must always be properly safeguarded. Property losses frequently occur because regulations relating to proper safeguarding and handling are not followed. Security is responsible for tracking material losses and identifying trends and areas where security enhancements may be required. To enhance the overall benefit of the program, both security personnel and inventory accuracy personnel need to work together in identifying losses and trends.
5. All MLSR or compromised classified material, equipment, repair parts, high risk AA&E will be reported by the cognizant department within 48 hours of incident discovery by utilizing the Operations Manual-3 Navy Blue (OPREP-3NB) format. This action eliminates a special message format used only for MLSR incidents and makes incident reporting format consistent throughout the Navy. The OPREP-3NB messages along with a preliminary inquiry are now used to report such incidents. An initial report will be submitted as soon as a loss or recovery of a reportable item is established.

NAVSUPINST 5530.1D
28 August 2001

The fact can be established by discovery of an incident, receipt of a loss claim, completion of an inventory or by any other means. The final MLSR reports in the formats prescribed will be submitted for all material upon completion of causative research, investigation or other inquiry.

6. The following items must be reported by OPREP-3NB message on all missing, lost, stolen or recovered material within 48 hours:

a. AA&E

- (1) One or more missile or rocket rounds;
- (2) One or more machine-guns;
- (3) 25 or more manually operated or semiautomatic weapons (includes revolvers and semiautomatic pistols);
- (4) One or more automatic fire weapons;
- (5) Ammunition as follows:
 - (a) Over 5,000 rounds (or 20,000 rounds of .38 caliber) or more of ammunition smaller than 40 millimeters (mm); five rounds or more of 40mm and larger ammunition; and
 - (b) Any fragmentation, concussion, or high explosive grenade including artillery or ground burst simulators, or other type of simulator or device containing explosive materials;
- (6) One or more mines (antipersonnel and antitank);
- (7) Demolition explosives including detonation cord, blocks of explosives (C-4), and other explosives.

b. Classified Equipment/Repair Parts

(1) All classified equipment/repair parts, excluding Communications Security (COMSEC) material. However, cryptographic items accountable within the COMSEC Material System are not included in the program except Controlled Cryptographic Items (CCI). Incidents involving CCI material in the supply system must be reported within 48 hours of discovery to Commander, Naval Security Group Command.

(2) Classified printed material losses are not included under this program and will be reported as prescribed in reference (d).

7. An example of an OPREP-3NB MLSR message is shown as Exhibit VIII-1.

8. The cognizant commanding officer is responsible for reporting a loss or compromise of classified material or high risk AA&E maintained on NAVSUP records. Commanding officers will ensure such incidents are properly investigated and the necessary actions are taken to negate or minimize the loss or compromise and to preclude recurrence.
9. The DD Form 200 (Financial Liability in Investigation of Property Loss) is no longer authorized for MLSR reporting. However, the DD Form 200 is still required and used for determining and assessing the amount of financial liability of those responsible for Government property lost, damaged or destroyed.
10. Upon discovery of lost classified notify your command security manager immediately. The command security manager will notify the local NCIS, ensure all reporting requirements are met and will provide other coordination that may be required (including the Defense Logistics Agency (DLA)).
11. The DON information security program regulation also requires a Preliminary Inquiry (PI). The PI is in addition to the OPREP-3NB message report. A PI is to be initiated and completed within 72 hours. The PI message or letter is sent to CNO (N09N2) with copies to NAVSUP 03X, the originator and the original classification authority of the lost or compromised material.
12. If the PI concludes a loss or compromise of classified material occurred or a significant command security weakness or vulnerability is revealed, the command shall immediately initiate a Judge Advocate General Manual investigation. All items listed in Appendix C other than classified material and high-risk ammunition will be reported utilizing the following (submission time frames are established by the applicable NAVSUP instructions):
 - a. DD Form 200
 - b. SF-364
 - c. SF-361
13. Security directors will review the completed DD Form 200, SF-364, and SF-361 to determine if an appropriate investigation has been conducted. Inventory and accountability losses must be investigated thoroughly in order to determine through investigation the loss was not the result of theft or misappropriation. On the DD Form 200, in block 10, indicate NCIS notification on all incidents involving theft or suspected theft.

NAVSUPINST 5530.1D
28 August 2001

On the SF-364, in block 12, indicate the date of NCIS notification on all incidents involving theft or suspected theft. On SF-361, in block 30, indicate NCIS notification on all incidents involving theft or suspected theft.

14. Each activity must evaluate the potential for pilferage throughout the command to include all partnership locations. Procedures will be developed to alleviate vulnerabilities. Security personnel should review documentation and visit facilities which receive, stow and ship material. Loss prevention statistics will be included in the activity's annual security report submitted by the director of security.

NAVSUPINST 5530.1D
28 August 2001

EXHIBIT VIII-1

FM USS NEVERSAIL
TO CNO WASHINGTON DC//N09N3//
NAVSURFWARCENDIV CRANE IN//4044//

INFO (Chain of command to include responsible command having custody at the time of loss or recovery, commanding officer of base(s), provost marshal (where item may have been lost/recovered))

BT

UNCLAS (OR AS APPROPRIATE)

MSGID/OPREP-3NB/NEVERSAIL/001/FEB//
FLAGWORD/NAVYBLUE/MLSR//
TIMELOC/020001ZFEB00/NORFOLK VA/INIT//
GENTEXT/INCIDENT IDENTIFICATION AND DETAILS/MLSR//
RMKS/

ACC: N12345/USS NEVERSAIL
RPT: 2000/007-INITIAL
AAA: VIRGINIA
BBB: A-93-12-20

CCC: 1. (1) ARMS (2) MISSING (3) M60 MACHINE GUN, 1 EA
(4) SACO INC. (5) 765432 (6) 1005-00-726-5661 (7) MACHINE GUN
M603 (8) 6,630.00 (9) 2 (10) ORD MAG 4LC-103 2. (1) AMMUNITION
(2) MISSING (3) 20MM CARTRIDGE, 5000 EA (4) HONEYWELL INC. (5)
B400 (6) 1305-00-028-6529 (7) CARTRIDGE, 20MM (8) 800.00 (9) 3
(10) ORD MAG 4LC-103

DDD: ACCOUNTABILITY: YES, LT W.T. DOOR, SSN: 123-45-6789

EEE: INVESTIGATION: NCIS NOTIFIED, S/A I.M.HARD, CASE
OPENED 00-01-13

FFF: SUMMARY: DURING INVENTORY OF ORD MAG 4LC-03 ON
01FEB00 ASSETS COULD NOT BE LOCATED. MACHINE GUN AND AMMUNITION
WERE IN SEPARATE BOXES BOUND BY METAL STRAPS. STRAPS WERE
BROKEN, NO SUPPORTING DOCUMENTATION. INVESTIGATION INTO CAUSE
IN PROGRESS. DOCUMENT NUMBER IS N60034-0012-B1328

GGG: POC: LT JOHN DOE, COMBAT SYSTEMS OFFICER, DSN
123-4567, COMM (123) 456-7890//

CHAPTER IX

COMMUNICATIONS SECURITY

1. The Commander, NAVICP will appoint a Communications Material Security Responsible Officer (CMSRO). The CMSRO will appoint a Communications Material Security (CMS) custodian and alternate custodian. The commanding officers of other NAVSUP activities, which do not have a CMS account, but do have STU-III secure telephones, will appoint a STU-III user representative and custodian. If the activity STU-III telephones are still under the NAVICP CMS account, efforts should be made to transfer custody to a local CMS account. This should be coordinated with the NAVSUP oversight CMS command authority. All NAVSUP personnel with CMS responsibilities will use the operating procedures in Attachment (1) for all matters not covered by references (w) and (x).
2. STU-III user representatives and custodians will be appointed at the supported sites having STU-III phones and will be the on-site presence for the custodian. The custodian is responsible for all inventories and program documentation. The material control user is responsible for day-to-day operation of phones, training, troubleshooting, key renewal and customer service. Materiel control users are not required to maintain inventories, account documentation or manuals. A headquarters command authority certified inspector will conduct account inspections.
3. Maintenance and operation of the STU-III will be provided to consolidated mail facilities to ensure proper operation and transmission of classified material.
4. Each command is responsible for ensuring their emergency plans include procedures for the STU-III telephones. This may entail notification of the responsible COMSEC agency and following its guidance.
5. COMSEC incidents or Practices Dangerous to Security (PDS) must be reported to the local account element (the account element your STU-III's are under) and NAVSUP 03XA, utilizing the forms required by your local element.

CMS STANDARD OPERATING PROCEDURES

Command authority will:

- a. Be available to activity personnel for command assist visit.
- b. Provide geographic unique information to custodian for inclusion in emergency action plan.

Custodian will:

- a. Maintain warehousing for excess STU-III units.
- b. Send STU-III unit by registered mail within 2 working days from receipt of request.
- c. Notify local elements of due dates for annual and semi-annual reports.
- d. Receive and distribute STU-III terminals according to the agreed-upon distribution plan.
- e. Brief users on the operation of terminals and make sure they sign the primary user registration form.
- f. Assign case control number for incident/PDS reports.

Alternate custodian (may be more than one) will be ready to administer the account in the absence of the custodian.

Local elements will:

- a. Request assist visits from command authority via the custodian.
- b. Be the on-site point of contact for users.
- c. Have functional knowledge of troubleshooting procedures, installations, maintaining and keying of units.
- d. Request additional terminals from custodians by fax or e-mail.
- e. Forward semiannual and annual reports to the custodian within 5 working days of request.
- f. Maintain on-site key transaction log. The respective custodian will assign transaction numbers by fax or e-mail.

NAVSUPINST 5530.1D
28 August 2001

g. Order keys from Key Management System (KMS) using KMS form L3769. The following procedures will be used:

(1) Complete order form and fax to NAVICP and maintain one copy in local element's file.

(2) When keys arrive, consult and comply with CMS 6, Article 660, then

(3) Call the custodian and request an incoming transaction number.

(4) Fax one copy to the custodian.

(5) Issue keys per CMS 6.

(6) Key unit in accordance with CMS 6, Article 805e.

(7) Brief user on procedures.

(8) Issue Crypto Ignition Key (CIK).

(9) Receive and distribute STU-III terminals according to the agreed upon distribution plan.

(10) Brief users on the operation of terminals and make sure they sign the primary user registration form.

(11) Maintain an inventory of CIK serial number, assigned users, locations and terminals and update every 6 months.

(12) Report PDSs to custodian within 3 hours of discovery of incident.

(13) Forward copy of local destruction report to custodian.

CHAPTER X

SECURITY EDUCATION, TRAINING AND BRIEFINGS

1. General

a. Commanding officers are responsible for security education in their commands ensuring time is dedicated for training and awareness.

b. In addition to DON training requirements, there may be additional NAVSUP/activity specific training and supporting region training.

2. Requirement

a. Physical Security. Reference (q) stresses the security responsibility of every member of the Navy and every civilian employee of the Navy in a continuous, vigorous physical security education program. To be an effective security program, including ATFP, it must be supported by a security education program for all hands.

(1) The security education program will include all pertinent aspects of physical security, law enforcement and loss prevention programs including those specifically related to force protection and antiterrorism.

(2) All personnel, military and civilian shall receive initial security instruction.

(3) Refresher security training shall be given to the extent necessary to ensure personnel remain mindful of and proficient in meeting their security responsibilities.

(4) Reference (q) specifies requirements for contract guards. Even though most of the NAVSUP activity contract guard forces have been transferred to Fleet region control, we must make sure those training requirements and any activity specific requirements are met. Those contracts for guard forces that are still internal to NAVSUP activities must be reviewed to ensure they meet the requirements of reference (q).

b. Personnel Security. Reference (a) requires each command handling classified information to establish and maintain an active security education program to instruct personnel, regardless of their position, rank or grade, in security policies and procedures. The purpose of the security education program is to ensure all personnel understand the need and procedure for protecting classified information.

NAVSUPINST 5530.1D
28 August 2001

(1) Security education must be provided and tailored to meet the needs of the command, as well as those of different groups within the command.

(2) The security manager must provide a command security education program meeting the minimum briefing requirements of reference (a).

c. Information Security. Reference (d) requires personnel receive the security education necessary to enable quality performance of their security functions. References (d) and (n) describe detailed training guidance concerning the execution of the DON's information security program.

APPENDIX A

REFERENCES

- (a) SECNAVINST 5510.30, Subj: DON Personnel Security Program
- (b) DOD 5200.2-R, Subj: Personnel Security Program
- (c) DODD 5200.2, Subj: DOD Personnel Security Program
- (d) SECNAVINST 5510.36, Subj: DON Information and Security Program Regulation
- (e) DODD 5200.1, Subj: DOD Information Security Program
- (f) DOD 5200.1R, Subj: DOD Information Security Program Regulation
- (g) DODD 5230.25, Subj: Withholding of Unclassified Technical Data from Public Disclosure
- (h) OPNAVINST 5510.161, Subj: Withholding Of Unclassified Technical Data from Public Disclosure
- (i) NAVSEAINST C5511.32A, Subj: Safeguarding of NPI
- (j) DOD 5220.22-R, Subj: Industrial Security Regulation
- (k) DODD 5220.22, Subj: DOD Industrial Security Program
- (l) DOD 5220.22-M, Subj: DOD Industrial Security Program Operating Manual
- (m) DODD 5230.20, Subj: Visits, Assignments, and Exchanges of Foreign Nationals
- (n) SECNAVINST 5510.34, Subj: Manual for the Disclosure of DON Military Information to Foreign Governments and International Organizations
- (o) SECNAVINST 5430.103, Subj: Missions and Functions of the Navy International Programs Office
- (p) SECNAVINST 5510.31, Subj: Policy and Procedures for Control of Foreign Disclosure in the DON
- (q) OPNAVINST 5530.14, Subj: DON Physical Security
- (r) DOD 5200.8-R, Subj: Physical Security Program
- (s) OPNAVINST 5580.1, Subj: DON Law Enforcement Manual

NAVSUPINST 5530.1D
28 August 2001

- (t) SECNAVINST 5530.4, Subj: Naval Security Force Employment and Operations
- (u) SECNAVINST 5510.13, Subj: Security Education and Training
- (v) OPNAVINST 5585.2B, Subj: DON Military Working Dog Program
- (w) CMS 21, Subj: Communications Security Material Systems Policy and Procedures for Navy Electronic KMS
- (x) CMS 6, Subj: STU-III COMSEC Material Management Manual
- (y) DOD 5100.76M, Subj: DOD Physical Security of Sensitive Conventional AA&E
- (z) SECNAVINST 5500.29, Subj: Use of Deadly Force and the Carrying of Firearms by Personnel of the DON in Conjunction with Law Enforcement, Security Duties and Personal Protection
- (aa) OPNAVINST 3591.1, Subj: Small Arms Training and Qualifications
- (ab) OPNAVINST 5530.13, Subj: DON Physical Security for Conventional AA&E
- (ac) NAVSEAINST 8370.2, Subj: Small Arms and Weapons Management Policy and Guidance Manual of 12 Jun 89
- (ad) DOD Directive 2000.12, Subj: DOD ATRFP Program
- (ae) DOD 0-2000.12H, Subj: DOD Protection of DOD Personnel Against Terrorist Acts
- (af) DODI 2000.14, Subj: DOD Combating Terrorism Program Procedures of 15 Jun 94
- (ag) DOD 0-2000.16, Subj: DOD Terrorism Program Standards
- (ah) CNO Washington DC 121050Z Feb 97, Subj: ATRFP Training and Certification
- (ai) SECNAVINST 3300.2, Subj: Combating Terrorism Program,
- (aj) OPNAVINST 3300.53, Subj: DON Combating Terrorism
- (ak) OPNAVINST 3300.54, Subj: Protection of Navy Personnel and Activities against Acts of Terrorism and Political Turbulence
- (al) NAVSUPINST PUB 723 Subj: Navy Inventory Integrity Procedures

NAVSUPINST 5530.1D
28 August 2001

- (am) NAVSUPINST 4440.146C, Subj: Safeguarding of DLA Sensitive Inventory Items Controlled Substances, and Pilferable Items of Supply
- (an) NAVSUPINST 4440.157, Subj: Material Turned into Store (MTIS) Manual
- (ao) NAVSUPINST 6710.1A, Subj: Requisitioning of Controlled Substances
- (ap) NAVMED MANUAL P117 (Chapter 21) (Pharmacy and Drug Control), Subj: Manual of Medical Department USN Reprint Includes Changes 1 through 113
- (aq) DOD 4525.8-M, Subj: DOD Official Mail Manual
- (ar) OPNAVINST 5218.7, Subj: Navy Official Mail Management Instruction
- (as) OPNAVINST 5218.1, Subj: OPNAV Mail Handling Procedures
- (at) DODD 5205.2, Subj: DOD Operations Security (OPSEC) Program
- (au) OPNAVINST 3432.1, Subj: OPSEC
- (av) OPNAVINST 3100.6G, Subj: Special Incident Reporting (OPREP-3, Navy Blue and Unit SITREP) Procedures

APPENDIX B

CONTROLLED INVENTORY ITEM CODES

1. This annex outlines some of the coding in various record fields, as well as material movement documents that will identify material irrespective of the NSN or nomenclature displayed. Knowing where this coding appears on documents is necessary to ensure material handlers properly secure and move the item. These codes may be used in conjunction with one another and with other fields; e.g., Controlled Inventory Item Codes (CIIC) and the demil code, cog and FSC, special material identification codes (SMIC), etc. Using this information and comparing with computer scans will indicate whether the materiel is properly stored, disposed of correctly or allow an item manager to know where it is stored.

2. CIIC: These codes are most commonly referred to as security and pilferage codes. It is a code indicating the materiel requires protection in the interest of national security, public safety or implies special precautions.

a. SECURITY CODES. (For classified, NNPI and CCI materiel)

<u>CODE</u>	<u>EXPLANATION</u>
A	Confidential - Formerly Restricted Data
B	Confidential - Restricted Data
C	Confidential
D	Confidential - Cryptologic
E	Secret - Cryptologic
F	Top Secret - Cryptologic
G	Secret - Formerly Restricted Data
H	Secret - Restricted Data
K	Top Secret - Formerly Restricted Data
L	Top Secret - Restricted Data
O	Item contains naval nuclear propulsion information; disposal and access limitations are identified in NAVSEAINST C5511.32.
S	Secret
T	Top Secret
7	Relates primarily to disposal process. Item displays/contains sensitive information.
9	This code identifies an item as a CCI

NOTE: Codes A, B, G and H should only relate to FSC 1100 and, within Navy, to selected 8A/0A cogs.

b. SENSITIVE CONVENTIONAL AA&E SECURITY RISK CODES.

Ordnance and related items with an unpacked unit weight of 100 pounds or less that must be carefully controlled due to combined factors of lethality, portability, utility and readiness for use. This type material also generally has a high dollar value and, in some cases, is very attractive to hostile governments and terrorists for its technical value and destructive capacity.

(1) Highest Sensitivity (Category I) - Non-nuclear missiles and rockets in a ready-to-fire configuration (e.g., Hamlet, Redeye, Stinger, Dragon, LAW, Viper) and explosive rounds for non-nuclear missiles and rockets.

(2) High Sensitivity (Category II) - AA&E

(3) Moderate Sensitivity (Category III) - AA&E

(4) Low Sensitivity (Category IV) - AA&E

(5) Highest Sensitivity (Category I) - AA&E with a security classification of Secret.

(6) Highest Sensitivity (Category I) - AA&E with a security classification of Confidential.

(7) High Sensitivity (Category II) - AA&E with a security classification of Confidential.

c. PILFERAGE CODE. A code indicating the material has a ready resale value of civilian application for personal possession and, therefore, is especially subject to theft.

<u>CODE</u>	<u>EXPLANATION</u>
I	Aircraft engine equipment and parts
J	Pilferable - Coding activities may further categorize pilferable items by using the following codes:
M	Hand tools and shop equipment
N	Firearms - This code should not appear on Navy materiel records. It is more appropriate to use Security Risk Codes 1 through 8 (less 7) for AA&E items.
P	Ammunition and explosives - This code should not appear on Navy material records. It is more appropriate to use Security Risk Codes 1 through 8 (less 7) for AA&E items.

- Q A drug or other controlled substance designated as a Schedule III, IV or V item, per the Controlled Substance Act of 1970. Other sensitive items requiring limited access storage.
- R Precious metals, a drug or other controlled substance designated as a Schedule I or II item, per the Controlled Substance Act of 1970. Other selected sensitive items requiring storage in a vault or safe.
- V Individual clothing and equipment.
- W For Navy managed items which have been identified through loss analysis and intelligence sources as especially vulnerable to theft. (For DLA and other service-managed items this code represents office machines.)
- X Photographic equipment and supplies.
- Y Communication/electronic equipment and parts.
- Z Vehicular equipment and parts.

3. SPECIAL MATERIEL CONTENT CODES (SMCC). These codes denote a physical characteristic of an item that will require special handling or safeguarding of the item. Those that demand the utmost attention are:

- a. Antibiotic
- b. Alcohol (ethanol, ethyl, alcohol or grain alcohol)
- c. Precious metals
- d. Medical kits
- e. Drugs (not Codes A, D, K or N)
- f. Narcotic
- g. Explosive non-ordnance items

NAVSUPINST 5530.1D
28 August 2001

h. High dollar value item. A high dollar value item is any item, except E and U, having three or more annual demand frequencies and an annual demand value of \$4,500 or more.

4. PRECIOUS METAL INDICATOR CODES. This code is used to identify items that have precious metals as part of their content. Indicator codes, except A, B and C, are to be included as selected items.

5. DLA INVENTORY CATEGORY CODE. H, E, U.

<u>Code</u>	<u>Explanation</u>
I	Critical and pilferable items. This includes security classified items, assemblages, serially numbered items and pilferable items.
J	Sensitive items--This includes narcotics, precious metals, drug abuse and medicinal spirits type items.

6. DEMILITARIZATION (DEMIL) CODE. This code has significance in that it delineates what actions are necessary and to what degree an item must be destroyed prior to release to a DRMO or prior to release to the general public via a DRMO sale. Of particular importance are codes C, D, E, F, G, N, P and, when established, V (vulnerable parts). Other codes are only significant if the item is to be disposed of overseas.

7. MATERIAL CONTROL CODES. Material Control Codes E, G, H, Q and X.

8. SPECIAL MATERIAL IDENTIFICATION CODES. Selected codes at sponsoring activity option are used in conjunction with other information to allow visibility of otherwise indeterminate commodities; i.e., indicates to which weapons system a part belongs. As examples: SS indicates a submarine-safety part, FK a field change kit, NI navigational, Q1 sonar pool, etc. Refer to NAVSUP Pub-437, Appendix 17, page 94, for listings.

9. WEAPONS. All FSC 10 materiel with Cog 6B or 6D.

APPENDIX C

CRITERIA FOR DESIGNATING AIS POSITION SENSITIVITY

The following is to be used as additional guidance to Chapter 5 of the SECNAVINST 5510.30A

SECNAVINST 5510.30A, Chapter 5 identifies AIS pertaining to position sensitivity. DOD Directive 5200.2R contains the following criteria for designating these positions and should be followed when designating AIS positions.

AIS I

- Responsibility or the development and administration of agency computer security programs and also including direction and control of risk analysis and/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsibility for the preparation or approval of data for input into a system which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement or authorization for disbursement from systems of;
 - (1) dollar amounts of \$10 million per year or greater, or
 - (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the AIS-I category to ensure the integrity of the system.
- Positions involving major responsibility for the direction planning, design, testing, maintenance, operation, monitoring and/or management of systems hardware and software.
- Other positions as designated by the agency head that involve relatively high risk for effecting grave damage or realizing significant personal gain.

NAVSUPINST 5530.1D
28 August 2001

AIS II

- Responsibility for systems design, operations, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the AIS I category, includes, but is not limited to:

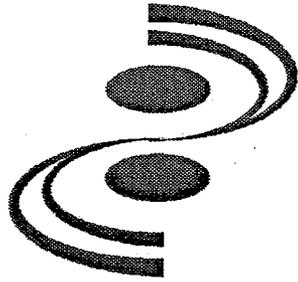
(1) Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving award of contracts;

(2) Accounting, disbursement or authorization for disbursement from systems of dollar amounts less than \$10 million per year. Other positions as designated by the agency head that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in AIS I positions.

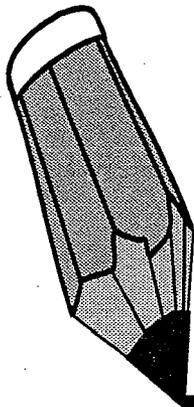
AIS III

- All other positions involved in Federal computer activities.

A Guide
for the
Preparation
of a
DD Form 254



National Classification
Management Society
Defense Security Service



Appendix D
To Enclosure (1)

Foreword

Introduction: The Federal Acquisition Regulation (FAR) requires that a DD Form 254 be incorporated in each classified contract. The DD Form 254 provides to the contractor (or a subcontractor) the security requirements and the classification guidance that would be necessary to perform on a classified contract.

Purpose: The purpose of this pamphlet is to assist Government Contracting Agency (GCA) personnel and prime contractors in their preparation of a DD Form 254. It contains step by step procedures for the filling out of the form. The instructions in the main body of the pamphlet correspond to the numbered items in the form. The back section of the pamphlet provides additional information related to the requirements for classified contracts, access considerations and terms and definitions.

Item 1. Clearance and Safeguarding.

1a. Facility Clearance Required

Insert the highest level of facility clearance required for the contractor to perform on the contract.

- It is not necessary to cite special categories of classified such as Restricted Data, COMSEC, SCI, etc.
- The contractor must have a valid facility clearance at least as high as the classification indicated. To verify the contractor's facility clearance, contact the DSS Central Verification Activity at (888) 282-7682 or log on to the DSS web site (www.dss.mil) and follow the instructions.

1b. Level of Safeguarding Required

Insert the highest level of safeguarding capability required for the contractor to perform on the contract.

- The classification level should not be higher than shown in Item 1a.
- If the contractor will not need to possess or store classified at the facility, enter "Not Applicable" or "None." (If this is the case, Item 11a. must be marked "Yes.")

Note: Individual items of the DD 254 are displayed for illustration purposes in accompaniment to the text. They are not intended to represent a cumulative DD 254.

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED
<i>SECRET</i>
b. LEVEL OF SAFEGUARDING REQUIRED
<i>SECRET</i>

Item 2. This Specification is for:

Insert an "X" into the appropriate box. Although information may be entered in more than one box, only one "X" should appear in Item 2.

2a. Prime Contract Number

- Used when a GCA issues guidance to the Prime Contractor. The issuing activity enters the contract number.

2b. Subcontract Number

- Used when there is a Prime/Subcontractor relationship. The contractor issuing the subcontract enters the subcontract number. The prime contract number must also be entered in 2a.
- If Item 11e. is marked "Yes" and the services to be performed do not apply to a specific contract (for example guard services or maintenance), enter the term "Multiple Contracts" in 2a instead of the prime contract number.

2c. Solicitation or other number

- Used for an RFP, RFQ, IFB or other solicitation, regardless of whether or not the bid package will contain classified information. The issuing activity enters the solicitation number and the date by which bids are due.

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		
X	a. PRIME CONTRACT NUMBER <i>DLAB001-98-S-0000</i>	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	Due Date (YYMMDD)

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		
	a. PRIME CONTRACT NUMBER <i>DLAB001-98-S-0000</i>	
X	b. SUBCONTRACT NUMBER <i>P00000000</i>	
	c. SOLICITATION OR OTHER NUMBER	Due Date (YYMMDD)

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)		
	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER <i>J98-7754-A</i>	Due Date (YYMMDD) <i>YYMMDD</i>

Item 3 This Specification Is:

Insert an "X" into the appropriate box. Although information may be entered in more than one box, only one "X" should appear in Item 3.

3a. Original

Original DD 254s are issued:

- For a solicitation for a classified contract, whether or not the actual bid package contains classified information.
- Upon the award of a classified contract
- Upon the award of a classified subcontract

The date of issuance is entered by the issuing activity.

3b. Revised

- When there is a change to classification guidance, a Revised DD 254 is issued. Give a sequential number to each revision and enter the date of the Revised DD 254.
- Enter the date of the Original DD 254 in 3a.

3. THIS SPECIFICATION IS: (X and complete as applicable)		
X	a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 990601
	b. REVISED (Supersedes all previous specs)	Revision No. Date (YYMMDD)
	c. FINAL (Complete Item 5 in all cases)	Date (YYMMDD)

3. THIS SPECIFICATION IS: (X and complete as applicable)		
	a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 990601
X	b. REVISED (Supersedes all previous specs)	Revision No. 1 Date (YYMMDD) 000228
	c. FINAL (Complete Item 5 in all cases)	Date (YYMMDD)

3c. Final

- When a Prime Contractor or a Subcontractor requests an extension of retention authority and it is approved by the GCA, a Final DD 254 may be issued to reflect this. (See NISPOM Chapter 5, Section 7 for more information on disposition and retention.)
- Enter the date the Final DD 254 is issued. Complete Item 5 as appropriate.
- Enter the date of the Original DD 254 in 3a.

Item 4. Is this a Follow-On Contract?

A Follow-On Contract is a contract that is let to the same contractor or subcontractor for the same item or services as a preceding contract. When this condition exists, mark "Yes" and enter the preceding contract number in the space provided. This item authorizes the contractor or subcontractor to transfer material received or generated under the preceding contract to the new contract. The material transferred should be reflected in Item 13.

Item 5. Is this a Final DD 254?

If this is a FINAL DD 254, mark "YES" and enter the date of the contractor's request for retention and the authorized period of retention in the spaces provided. If this is not for a FINAL, mark "NO."

3. THIS SPECIFICATION IS: (X and complete as applicable)		
	a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 990601
	b. REVISED (Supersedes all previous specs)	Revision No. Date (YYMMDD)
X	c. FINAL (Complete Item 5 in all cases)	Date (YYMMDD) 050201

4. IS THIS A FOLLOW-ON CONTRACT? YES NO If Yes, complete the following:
 Classified material received or generated under DNA001-99-C-100 (Preceding Contract Number) is transferred to this follow-on contract.

4. IS THIS A FINAL DD FORM 254? YES NO If Yes, complete the following:
 In response to the contractor's request dated 991231, retention of the identified classified material is authorized for the period of 2 years.

Item 6. Contractor

Used when a GCA issues guidance to a Prime Contractor.
Enter information as follows:

- 6a. Name and address of the contractor
 - 6b. The contractor's CAGE code
 - 6c. The appropriate CSO and address
- (For CSO addresses, see Appendix A of NISPOM or contact your local DSS office for updated information.)

Item 7. Subcontractor

If the DD 254 is for a subcontract, enter information as follows:

- 7a. Name and address of the subcontractor
 - 7b. The subcontractor's CAGE code
 - 7c. The appropriate CSO and address
- Items 6a, 6b and 6c may be left blank.

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)		
<p>a. NAME, ADDRESS, AND ZIP CODE</p> <p>ABC Corp. P.O. Box 12345 Wayne, PA 19087</p>	<p>b. CAGE CODE</p> <p>21732</p>	<p>c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)</p> <p>DSS Mail Stop 5 Intnat'l Plaza II, #445 Philadelphia, PA 19113</p>

7. SUBCONTRACTOR		
<p>a. NAME, ADDRESS, AND ZIP CODE</p> <p>XYZ Corp. 123 Wilson Ave. Huntsville, AL 35802</p>	<p>b. CAGE CODE</p> <p>79986</p>	<p>c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)</p> <p>DSS 2300 Lake Park Dr. Suite 250 Smyrna, GA 30080 s</p>

Item 8. Actual Performance

If the work is to be performed at a location other than specified in Item 6a (or 7a, as appropriate), enter information as follows:

- 8a. Facility name and address
- 8b. the CAGE code of the facility where the work will be performed.
- 8c. The appropriate CSO and address
 - If the place of performance is the same as 6a (or 7a), either enter the facility's name or enter "Same as Item 6a (or 7a) in block 8a.
 - If there are more places of performance, identify them in Item 13. Include the facility name, address and CAGE code and send a copy of the DD 254 to the appropriate CSO(s).
 - Performance of a contract on government facilities should be explained in Item 13.

Item 9. General Identification of This Procurement

Enter a short, concise, and unclassified description of the procurement action. The action could be research, development, production, study, services, etc.

8. ACTUAL PERFORMANCE		
<p>a. NAME, ADDRESS, AND ZIP CODE</p> <p>HiTech Inc. 444 Main St. Richmond, VA 23233</p>	<p>b. CAGE CODE</p> <p>3L069</p>	<p>c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)</p> <p>DSS Pembroke Five Suite 525 Virginia Beach, VA 23462</p>

Note: If inspections will be conducted by an organization other than the CSO, complete Item 15. Inspections by an agency other than the CSO does not change the CSO designation and does not relieve the contracting activity from the responsibility of providing a copy of the DD 254 to the CSO.

<p>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Research and Development of Countermeasures Against Grayhawk Missile.</p>

Item 10. This Contract Will Require Access To:

Mark all items "YES" or "NO," as appropriate to the requirements of the contract. (Coordinate with the appropriate program and other security offices to ensure the proper types of access are imposed on the contractor or subcontractor.) An explanation of each item follows.

10.a. Communications Security Information

COMSEC information includes accountable or non-accountable COMSEC information and controlled cryptographic items (CCI).

- If accountable COMSEC material is involved, the contractor must have a COMSEC account and item 11h must be marked "YES."
- Prior approval from the GCA is required in order for a Prime Contractor to grant COMSEC access to a subcontractor. The Prime Contractor should also notify the NSA Central Office of Record (COR) before negotiating or awarding subcontracts.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	
b. RESTRICTED DATA		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		
d. FORMERLY RESTRICTED DATA		
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)		
(2) Non-SCI		
f. SPECIAL ACCESS INFORMATION		
g. NATO INFORMATION		
h. FOREIGN GOVERNMENT INFORMATION		
i. LIMITED DISSEMINATION INFORMATION		
j. FOR OFFICIAL USE ONLY INFORMATION		
k. OTHER (Specify)		

10.b. Restricted Data

Mark "YES" if access to RESTRICTED DATA information is required under the contract.

- 10b must be marked "YES" if item 10c is marked "YES."

10.c. Critical Nuclear Weapon Design Information

Mark "YES" if access to CNWDI is required under the contract.

- GCA approval is required prior to granting CNWDI access to a subcontractor.

10.d. Formerly Restricted Data

Mark "YES" if access to FORMERLY RESTRICTED DATA is required.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		
b. RESTRICTED DATA	X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	X	
d. FORMERLY RESTRICTED DATA	X	
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)		
(2) Non-SCI		
f. SPECIAL ACCESS INFORMATION		
g. NATO INFORMATION		
h. FOREIGN GOVERNMENT INFORMATION		
i. LIMITED DISSEMINATION INFORMATION		
j. FOR OFFICIAL USE ONLY INFORMATION		
k. OTHER (Specify)		

10.e. Intelligence Information

The Director of Central Intelligence (DCI) has jurisdiction and control of intelligence information. If intelligence information must be accessed, the GCA is responsible for ensuring that the additional security requirements outlined in various DCI Directives are incorporated in the guidance provided to the contractor. (The CSO does not conduct security reviews for SCI but is still responsible for security reviews involving NON-SCI in the possession of a contractor or subcontractor.)

If access to SCI is required:

- Mark 10e(1) "YES."
- Mark Items 14 and 15 "YES."

If access to non-SCI is required:

- Mark 10e(2) "YES."
- Mark Item 14 "YES"
- Mark Item 15 "NO."

If access to SCI and non-SCI is required:

- Mark 10e(1) and 10e(2) "YES."
- Mark Item 14 "YES."
- Mark Item 15 as appropriate

Prior approval of the GCA is required before a subcontract involving access to Intelligence Information can be issued.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		
b. RESTRICTED DATA		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		
d. FORMERLY RESTRICTED DATA		
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)	X	
(2) Non-SCI		
f. SPECIAL ACCESS INFORMATION		
g. NATO INFORMATION		
h. FOREIGN GOVERNMENT INFORMATION		
i. LIMITED DISSEMINATION INFORMATION		
j. FOR OFFICIAL USE ONLY INFORMATION		
k. OTHER (Specify)		

10.f. Special Access Information

Special Access Programs (SAPs) impose requirements on the contractor that exceed the NISPOM. When SAP information is involved, the Program Security Office of the GCA is responsible for providing the contractor with the additional security requirements needed to ensure adequate protection of the information. The additional requirements would be included in the contract document itself or Item 13 or both.

If SAP requirements are imposed on the contractor:

Mark 10f "YES."

Mark Item 14 "YES."

Complete Item 15 as appropriate. (Some SAPs qualify as carve-outs, but not all SAPs are carve-outs.)

If a SAP subcontract is awarded, it is the prime contractor's responsibility to incorporate the additional security requirements in the subcontract. Authority for access must be obtained from the Program Security Office of the GCA.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		
b. RESTRICTED DATA		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		
d. FORMERLY RESTRICTED DATA		
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)		
(2) Non-SCI		
f. SPECIAL ACCESS INFORMATION	X	
g. NATO INFORMATION		
h. FOREIGN GOVERNMENT INFORMATION		
i. LIMITED DISSEMINATION INFORMATION		
j. FOR OFFICIAL USE ONLY INFORMATION		
k. OTHER (Specify)		

10.g. NATO Information

Mark "YES" if the contract requires access to information or documents belonging to the NATO.

The Prime contractor must receive approval from the GCA to grant NATO access to a subcontractor.

10.h. Foreign Government Information

This item includes any foreign government information except NATO. Mark "YES" if applicable.

The Prime contractor must receive approval from the GCA to grant access to a subcontractor.

10.i. Limited Dissemination Information (LIMDIS)

This is no longer a valid program and you should not have any new documents or contracts reflecting this caveat. Until the DD 254 is revised, this block should be marked "NO."

10.j. For Official Use Only Information

This item may be applicable on some classified contracts. When this item is marked "YES," the GCA is responsible for providing the contractor with the safeguards necessary for the protection of the information. The NISPOM does not provide guidance concerning FOUO so the GCA must provide guidance on protection procedures in Item 13.

10.k. Other

Use this item for any other information not included in 10a through 10j. Specify the type of information and include any additional remarks in Item 13.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		
b. RESTRICTED DATA		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		
d. FORMERLY RESTRICTED DATA		
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)		
(2) Non-SCI		
f. SPECIAL ACCESS INFORMATION		
g. NATO INFORMATION	X	
h. FOREIGN GOVERNMENT INFORMATION	X	
i. LIMITED DISSEMINATION INFORMATION		X
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER (Specify) See Item 13	X	

Item 11. In Performing This Contract, the Contractor Will:

Mark all items "YES" or "NO" according to the requirements of the contract. (Coordinate with program and other security offices to ensure the appropriate controls are imposed on the contractor or subcontractor.) An explanation of each item follows.

11.a. Have access to classified information only at another contractor's facility or at a government activity.

"ONLY" is the key word. Mark "YES" when access or storage of classified information is not required at the contractor's facility.

If marked "YES,":

- Item 1b should be marked "N/A" or "None."
- The following annotation may be added in Item 13: "Contract performance is restricted to (enter name and address of contractor facility (cage code), or Government Activity)."

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X	
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.b. Receive classified documents only.

“ONLY” is the key word. Mark “YES” when the contractor will receive classified documents (instead of classification guides) in order to perform on the contract but is not expected to generate classified information. The classification markings shown on the documents received will provide the classification guidance necessary.

- Although the contractor is not expected to generate classified information in this scenario, sometimes a change in circumstances causes a situation where the contractor needs to generate some classified materials. In order to afford flexibility for such situations, the following annotation may be added in Item 13: “Any classified information generated in the performance of this contract shall be classified according to the markings shown on the source material.”

If the volume or configuration of the documents is such that specialized storage requirements are necessary, contact the CSO to verify storage capacity at the contracting facility.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY	X	
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.c. Receive and generate classified information.

Mark "YES" when the contractor is expected to receive and generate classified material (documents and/or hardware) and will require detailed security classification guidance in order to perform on the contract.

If this item is marked "YES," detailed security classification guidance must be provided. The guidance may be:

- Included in Item 13, and/or
- Attached to the DD 254, and/or
- Forwarded under separate cover, and/or
- Included in the contract document itself.

If the volume or configuration of the documents is such that specialized storage requirements are necessary, contact the CSO to verify storage capacity at the contracting facility.

Appropriate statements may be included in Item 13 to direct the contractor to the guidance for the contract.

11.d. Fabricate, modify, or store classified hardware.

Mark "YES" if the contractor is expected to generate or utilize hardware containing classified.

Include as much information as possible (additional information can be added in Item 13) to describe the nature and extent of the storage that will be required.

- Will Restricted or Closed Areas will be required?
- How much hardware is involved? How Large?

If more than 2 cubic feet of storage is required, contact the CSO to verify storage capacity at the contracting facility.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.e. Perform services only.

Mark "YES" if the contractor is performing a service only and is not expected to produce a deliverable item.

You should enter a statement in Item 13 that explains the services and that provides appropriate security guidance. Some examples are provided below.

Graphic Arts Services

"Reproduction services only. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this contract."

Engineering Services

"Contract is for engineering services. Classification markings on the material to be furnished will provide the classification guidance necessary for the performance of this contract."

Equipment Maintenance Services

"Contract is for equipment maintenance services on equipment which processes classified information. Actual knowledge of, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because access to classified information can not be precluded by escorting personnel. Any classification guidance needed will be provided by the contractor."

Guard Services

"Contract is for guard services. Cleared personnel are required by the NISPOM to provide supplemental protection."

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY	X	
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.f. Have access to U.S. classified information outside the U.S., Puerto Rico, U.S. Possessions and Trust Territories.

If "YES," indicate in Item 13 the U.S. activity where the overseas performance will occur. Also list the city and country. Item 14 may also be marked "YES" and completed as appropriate depending upon the programs involved. Because security reviews will have to be conducted by an organization other than the CSO, Item 15 should also be completed as appropriate.

- For DoD contractors performing on overseas contracts, provide a copy of the DD 254 to the appropriate DSS Office of Industrial Security, International. (See NISPOM Appendix A or contact DSS.)
- See NISPOM paragraph 10-204 for suggested "Security Clauses for International Contracts" for classified contracts involving foreign contractors.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X	
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.g. Be authorized to use the services of the Defense Technical Information Center (DTIC) or other secondary distribution center.

Mark "YES" if the contractor is to be authorized use of DTIC services. DD Form 1540 and DD Form 2345 must be completed for registration with DTIC.

- The sponsoring GCA submits the DD Form 1540 "Registration for Scientific and Technical Information Services" to DTIC on behalf of the contractor. For subcontractors, the prime contractor submits the DD 1540 with the GCA verifying need to know.
- The contractor may also submit DD Form 2345 "Militarily Critical Technical Data Agreement" (after registration with DTIC) to the Defense Logistics Services Center for access to unclassified, militarily critical technical data from other DoD sources. The GCA must certify the need-to-know to DTIC.
- See NISPOM Chapter 11, Section 2 for more information.

11.h. Require a COMSEC account.

Mark this item "YES" if accountable COMSEC information must be accessed in the performance of the contract. If non-accountable COMSEC information is involved, mark this item "NO."

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
h. REQUIRE A COMSEC ACCOUNT	X	
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.i. Have TEMPEST Requirements.

Mark "YES" if the contractor is required to impose TEMPEST countermeasures on information processing equipment after vulnerability assessments are completed.

TEMPEST requirements are additional to the requirements of the NISPOM. Thus, Prime Contractors may not impose TEMPEST requirements on their subcontractors without GCA approval.

- If marked "YES," Item 14 must also be marked "YES" and pertinent contract clauses identified or added to Item 13.
- If requested by the GCA, TEMPEST Countermeasure Assessment Requests may be included as an attachment to the DD 254.

11.j. Have Operations Security (OPSEC) Requirements.

Mark "YES" if the contractor must impose certain countermeasures directed to protect intelligence indicators.

OPSEC requirements are additional to the requirements of the NISPOM. Thus, contractors may not impose OPSEC requirements on their subcontractors unless the GCA approves the OPSEC requirements.

- If marked "YES," Item 14 must also be marked "YES" and pertinent contract clauses identified or added to Item 13.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS	X	
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
l. OTHER (Specify)		

11.k Be authorized to use the Defense Courier Service (DCS)

A "YES" in this block authorizes the contractor to use the services of DCS. The GCA must obtain written approval from the Commander, Defense Courier Service, Attn: Operations Division, Fort George G. Meade, MD. 20755-5370. Only certain classified information qualifies for shipment by DCS. The GCA is responsible for complying with DCS policy and procedures. Prior approval of GCA is required before a Prime Contractor can authorize a subcontractor to use the services of DCS.

11.l. Other (Specify)

Use this item to add any additional performance requirements not covered above. Item 13 should be appropriately annotated to provide any necessary remarks.

Item 12. Public Release

The contractor is responsible for obtaining the approval of the contracting activity prior to release of any information received or generated under the contract, except for certain types of information authorized by the NISPOM.

GCAs should complete this item as required by internal agency directives to direct the Prime Contractor to the appropriate office in the GCA that has public release authority. Prime Contractors should refer their subcontractors to the GCA office that was referenced in the Prime Contract DD 254.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. PERFORM SERVICES ONLY		
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
h. REQUIRE A COMSEC ACCOUNT		
i. HAVE TEMPEST REQUIREMENTS		
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
l. OTHER (Specify) See Item 13	X	

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

Direct
 Through (Specify):

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.

* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

Item 13. Security Guidance

Use this block to expand or explain information referenced other sections of the DD 254. When completing Item 13 consider these questions:

- What classified information will the contractor need in the performance of this contract?
- Is there an existing Security Classification Guide for the Program?
- If subcontracting, is the guidance in the Prime Contract DD 254 adequate? Does the entire Prime Contract DD 254 apply to the subcontract or do you only need to provide applicable portions?
- Will classified source documents be used? If so, do they contain all the guidance the contractor needs?
- What will the contractor's actual performance be? (e.g., R&D, Test, Production, Study, etc.?)
- What unique characteristics are involved that need protection? Are there design features which require protection? Is there technical information which will require protection?
- What breakthroughs would be significant if achieved in an R&D effort?
- Are there performance limitations that require protection?
- Will classified hardware be furnished to or generated by the contractor?

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

- What information makes the hardware classified?
- Will hardware being generated require classification? At what stage in its production does it become classified?

These are some of the questions that should be asked when preparing guidance for a contractor. Put yourself in their place, do you understand the guidance? Will they?

Be sure to:

- identify the specific information to be classified
- provide appropriate downgrading or declassification instructions, and
- provide any special instructions, explanations, comments or statements necessary to clarify other items identified in the DD 254.

Factors to consider when completing Item 13 include:

Each contract is unique in its performance requirements. A standardized format may not necessarily be the best for every DD 254.

Give reasons for classification.

Write the guidance in plain English so it can be easily understood. Use additional pages to expand or explain guidance.

Be as specific as possible and include only that information that pertains to the contract for which it is issued.

Avoid references to internal directives and instructions. If such documents provide guidance applicable to the contract, extract the pertinent portions and provide them as attachments. All documents cited in Item 13 should be provided to the contractor, either as attachments or forwarded under separate cover.

Do not extract the requirements of the NISPOM or its supplements and include them in a DD 254. The NISPOM provides safeguarding requirements and procedures for classified information, not classification guidance.

Encourage participation by the contractor in the preparation of the guidance and submission of comments and/or recommendations for changes in the guidance that has been provided.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

Item 14. Additional Security Requirements

Complete this item whenever security requirements are imposed on a contractor that are in addition to the requirements of the NISPOM or its supplements.

Additional requirements translate into additional costs so it is essential that you coordinate with program and other security offices to ensure you are imposing appropriate requirements on the contractor.

- A “Yes” in this item requires the GCA or prime contractor to incorporate the additional requirements in the contract itself or to incorporate the additional requirements by statements or reference in Item 13.
- Costs incurred due to additional security requirements are subject to negotiation between the contractor and the GCA.
- Prior approval of the GCA is required before a prime contractor can impose additional security requirements on a subcontractor.
- A copy of the DD 254 containing the additional security requirements should be provided to the CSO.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use item 13 if additional space is needed.)

Yes

No

Item 15. Inspections

Mark "YES" if the CSO is relieved, in whole or in part, of the responsibility to conduct security reviews and provide security oversight to the contractor. Information should be provided regarding the specific areas from which the CSO is excluded and the agency that will assume the responsibility.

The CSO is relieved of the responsibility to inspect:

- SCI material. When access to SCI is required (Item 10.e.(I)), the following statement must be added: "(Enter appropriate Agency/Military Department Senior Intelligence Officer) has exclusive security responsibility for SCI classified material released or developed under this contract and held within the contractor's SCIF."
- Special Access Programs where the Program Security Office has "carved out" the CSO from inspection responsibility. Not all SAPs are "carve outs" because in some instances the Program Security Office will allow the CSO to retain inspection responsibility.
- Contractor facilities operating on military installations when the installation commander has elected to retain security cognizance.

In all cases, provide the CSO a copy of the DD 254.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas of elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

Yes

No

Item 16. Certification and Signature

Enter the name, title, telephone number, address and signature of a designated official certifying that the security requirements are complete and adequate for performance of the classified contract.

- The individual signing the DD 254 should ensure it has been adequately staffed among the appropriate contracting, program and security personnel.

Item 17. Required Distribution

Distribute copies of the DD 254, as appropriate, and indicate the distribution in the respective blocks. Additional copies can be distributed internally to your visit control office, contracts department, department heads, etc.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
d. ADDRESS (Include Zip Code)		
e. SIGNATURE		

17. REQUIRED DISTRIBUTION

<input type="checkbox"/>	a. CONTRACTOR
<input type="checkbox"/>	b. SUBCONTRACTOR
<input type="checkbox"/>	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
<input type="checkbox"/>	d. US ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
<input type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input type="checkbox"/>	f. OTHERS AS NECESSARY

Why do we use a DD 254 in a classified contract?

The Security Agreement (DD 441), executed between the government and all cleared facilities under the NISP, obligates the Government to provide the contractor appropriate classification guidance for the protection of the classified information, furnished to or generated by, the contractor in the performance of a classified contract.

The Government fulfills this obligation by incorporating a "Security Requirements Clause" and a DD 254 in each classified contract. The "clause" identifies the contract as a "classified contract" and the DD 254 provides classification guidance.

The DD 254 is a contractual specification. It is as important as any other specification in a contract. It is the vehicle that provides the contractor with the security classification guidance necessary for the classified information to be received and generated under the contract.

It was developed as a contractual document to capture in one place all of the security requirements for a classified contract. By checking the blocks for the preprinted items on the DD 254, the issuer provides the contractor with a brief summary of the security requirements that apply to the contract.

Pre-Award Considerations

Before a GCA or Prime Contractor issues a solicitation for a classified contract a determination should be made as to whether or not access to classified will be required during the solicitation process.

If access is not required during the solicitation process:

Prospective contractors do not have to possess facility clearances to bid on the solicitation. Only the successful bidder will be required to have a facility clearance and that will not be necessary until the contract is awarded.

If access *is* required during the solicitation process:

All prospective contractors must possess the appropriate facility clearance and safeguarding capability in order to access the solicitation package.

To determine the current clearance status of all prospective contractors, contact the DSS Central Verification Activity at (888) 282-7682 or log on to the DSS web site (www.dss.mil) and follow the instructions.

If any of the prospective contractors do not have the appropriate facility clearance, contact DSS and furnish, in writing, appropriate information needed to sponsor the clearance. The DSS Operations Center-Columbus (formerly DISCO) routinely issues Interim facility clearances at the SECRET or CONFIDENTIAL levels if the contractor is qualified.

Definitions

Classified Contract - Any contract, subcontract, purchase order, lease agreement, service agreement, etc., that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be classified even though the contract document is not classified.) This term is used throughout the NISPOM because it is the most common situation where a contractor has access to or possession of classified information. However, the requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Agency program or project which requires access to classified information by the contractor.

Classified Information - Any information that is owned by, produced by or for, or under the control of the U.S. Government, and determined pursuant to Executive Order 12958, or prior orders, to require protection against unauthorized disclosure, and is designated as TOP SECRET, SECRET or CONFIDENTIAL.

Cleared Contractor - Any corporation, company, contractor, consultant, individual or their employees, agents, representatives (actual or potential) who requires or will require access to classified information in the performance of a contract.

CNWDI - Critical Nuclear Weapon Design Information. A DoD category of weapon data designating TOP SECRET Restricted Data or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munition, or test device.

COMSEC - Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

Facility Clearance - An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category and all lower categories.

Final DD 254 - A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to provide classification guidance and security requirements to contractors who wish to retain classified information beyond the terms of the contract as authorized by the NISPOM.

Foreign Government Information - Information that is:

- a. Provided to the U.S. by a foreign government or governments, an international organization or government, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or
- b. Produced by the U.S pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments or any element thereof requiring that the information, the arrangement, or both are to be held in confidence.

Formerly Restricted Data - Classified information jointly determined by the DoE and its predecessors and the DoD to be related primarily to the military utilization of atomic weapons and removed by the DoE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

For Official Use Only - Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552.

NATO Information - Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside of NATO.

OPSEC - Operations Security. A security discipline designed to identify and analyze intelligence indicators which may have a bearing on the security integrity of a classified program.

Original DD 254 - A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to provide original classification guidance and security requirements on a classified contract. Original DD 254s are issued during the solicitation phase of a contract to provide classification guidance and security requirements to prospective contractors as they formulate their bids. Once the contract is awarded, another Original DD 254 is issued to the contractor who is being awarded the contract.

Prime Contract - A contract let by a GCA to a contractor for a legitimate government purpose.

Prime Contractor - Any contractor who has received a prime contract from a Government Agency. For purposes of subcontracting, a subcontractor shall be considered to be a prime contractor in relation to its subcontractor.

Restricted Data - All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

Revised DD 254 - A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to change classification guidance and security requirements on a classified contract.

SAP - Special Access Program. Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET OR CONFIDENTIAL information. A special Access Program can be created or continued only as authorized by the Deputy Secretary of Defense pursuant to E.O. 12958.

SCI - Sensitive Compartment Information. All Intelligence information and material that requires special controls for restricted handling within compartmented channels and for which compartmentation is established.

Subcontract - A contract entered into by a contractor to furnish supplies or services for performance of a prime contract or other subcontract.

Subcontractor – A supplier, distributor, vendor or firm that furnishes supplies or services to or for a prime contractor.

TEMPEST - An unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

ACRONYMS

CAGE	Commercial And Government Entity
CNWDI	Critical Nuclear Weapon Design Information
COMSEC	Communications Security
CSO	Cognizant Security Office
CVA	Central Verification Activity
DCI	Director of Central Intelligence
DCS	Defense Courier Service
DD	Defense Department
DSS	Defense Security Service
DTIC	Defense Technical Information Center
FOUO	For Official Use Only
FRD	Formerly Restricted Data
GCA	Government Contracting Agency
IFB	Invitation for Bid
IR&D	Independent Research and Development
LIMDIS	Limited Distribution
NATO	North Atlantic Treaty Organization
NISPOM	National Industrial Security Program Operating Manual
OISI	Office of Industrial Security International
OPSEC	Operations Security
PSO	Program Security Officer
RD	Restricted Data
RFP	Request For Proposal
RFQ	Request For Quote
SAP	Special Access Program
SCI	Sensitive Compartmented Information
TCAR	TEMPEST Countermeasure Assessment Request

APPENDIX E

MAIL CENTER SECURITY

1. All personnel are responsible for preventing the theft, misuse, waste or loss of postage stamps. Postage stamps shall be secured in locked containers or in a locked room.

2. Meter Security

a. Meters

(1) Secure a meter with an access code or remove the meter, and place it in a locked safe, file cabinet or in a locked room overnight and any other time the operator is temporarily absent and adequate surveillance cannot be maintained to prevent unauthorized use of the meter.

(2) Immediately report the loss, theft and recovery of a lost or stolen meter to the local post office, the equipment vendor and through command channels to the DOD Official Mail Manager, Military Postal Service Agency, 2461 Eisenhower Avenue, Suite 812, Alexandria, VA 22331-0006. Reports shall include the meter make, model and serial number; the date, location and details of the loss, theft or recovery; and a copy of the police report when applicable.

b. Meter Access Codes

Only the supervisor or other personnel authorized by the supervisor should have knowledge of the access code used to operate and/or reset the meter. When unauthorized personnel become knowledgeable of the access code the supervisor must immediately change the code.

3. Registered Mail

a. Registered mail must be kept separate from other accountable mail. Mail centers that accept, receive and store registered mail shall designate a secure area or have a separate registry section and the registered mail must be secured in a safe.

b. Registered mail, if held overnight, must be locked in a GSA-approved safe.

4. Security of the Mail

a. Mail handling areas and all receptacles for accountable mail shall be locked when responsible individuals are not physically present.

NAVSUPINST 5530.1D
28 August 2001

b. Official registered mail stored overnight will be safeguarded in an approved security container that meets the requirements for storing secret material.

c. Structural requirements for mail centers that store official registered mail or personal mail overnight are as follows:

(1) Doors shall be provided with suitable locks and door hinges shall be mounted inside to prevent their removal from the outside.

(2) Windows easily accessible from the outside shall be barred. Other windows shall be covered with heavy wire mesh.

(3) Walls and ceilings shall be constructed of material that prevents forcible entry.

(4) Receptacles, when used, shall be installed to prevent access to other receptacles or access from a customer service window.

d. Access shall be limited to those personnel conducting official business at the facility, including designated mail clerks, mail orderlies, postal clerks, officers, enlisted members and civilians on official inspections and visits. Maintenance personnel and work details shall be allowed access only when escorted or under constant surveillance by mail center employees.

e. Combinations of containers used to store registered mail shall be changed annually, when there is a change of the clerk responsible for the container and when an actual or suspected compromise occurs.

5. Qualifications of mail center employees.

a. Possess a high degree of honesty and be trustworthy.

b. Never been convicted of crimes involving theft.

c. Not been previously removed for cause from work in a postal facility or other mail activity.

d. Not have physical restrictions prohibiting duty involving prolonged standing, walking, or lifting weights up to and including the maximum weight for a mail piece.

e. Possess a valid civilian driver's license when duties require driving.

f. Must be eligible for at least a secret clearance. This is determined by having a favorable entrance NAC or NAC on file.

6. Temporary employees such as summer hires may be used in a limited role. Because these employees normally do not have a security clearance they cannot handle accountable items or open first-class or priority mail. They must work under the physical supervision of a full time mail center employee.

7. Unit mail clerks or mail orderlies who receive mail from a mail center must meet the requirements of the DOD Postal Manual, Volume II. Foreign nationals may be appointed as unit mail clerks or mail orderlies provided all requirements of the DOD Postal Manual, Volume II are complied with. However, foreign nationals cannot receipt for or handle official registered mail.

8. Transporting Mail

a. A closed-body vehicle equipped with lockable doors shall be used to transport mail to-and-from mail service areas. Mail being transported in other than a closed-body vehicle shall be accompanied by a guard who will ride in the truck body with the mail or the guard will be positioned to maintain visual contact with the mail at all times. Mail will always be protected from the elements.

b. Privately owned vehicles may not be used to transport mail.

9. Mail center managers will establish and conduct a program to train all mail center employees. This includes annual mail bomb training to all personnel who process mail. Your local security department can assist in providing or arranging for the required training.