OPNAV-M 5510.1
DNS-34
28 Aug 2017

OFFICE OF CHIEF OF NAVAL OPERATIONS SECURITY REGULATIONS MANUAL

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON DC 20350-2000

OPNAV-M 5510.1
DNS-34
28 Aug 2017

FOREWORD

This manual implements the policy set forth in the Office of the Chief of Naval Operations Instruction 5510.60N (OPNAVINST 5510.60N). It provides security policy direction while delineating standardized procedural guidance for the protection of classified information and Controlled unclassified information (CUI) in the custody of the Chief of Naval Operations (CNO), the Office of the Chief of Naval Operations (OPNAV) staff or other Metro Washington, DC, offices for which the CNO has cognizance for security. This manual, which is effective immediately, is mandatory and applicable to the immediate offices of the Chief of Naval Operations to ensure maximum uniformity and effectiveness in the application of security program policies as carried out by the OPNAV Security serviced activities under the guidance of the OPNAV Security Manager.

This manual is detailed guidance for military, civilian personnel, and supporting contractors as delineated by the President Executive Order 13526, 29 Dec 2009

Local supplements and subordinate operations procedures will not contradict or simply repeat information contained in this manual but will clearly define additional details of command unique requirements.

Forward recommended changes to this manual to:
Chief of Naval Operations
Director, Navy Staff
DNS-34 (OPNAV Security Manager)

Alphonso W. Moore

TABLE OF CONTENTS

CHAPTER 1
GENERAL REGULATIONS AND ORGANIZATIONS

1. Purpose. To provide security policy and procedural guidance under the mandates of references (a) through (u) for the protection of classified information and controlled unclassified information (CUI) in the custody of the Chief of Naval Operations (CNO), the Office of the Chief of Naval Operations (OPNAV) staff or other Metro Washington, DC, offices for which the CNO has cognizance for security.

2. Objective. To standardize mandated security operations and procedures for security serviced activities under the cognizance of the Chief of Navy Operations to ensure effective information, industrial, physical and personnel security program policies managed by the OPNAV Security Manager.

3. Each OPNAV Security Serviced Activity Must:

a. Appoint an individual per reference (c) to serve as the Security Coordinator and, as required, appoint Assistant Security Coordinators (exhibits 1A and 1B).

b. Designate Top Secret Control Officer (TSCO) and, Assistant Top Secret Control Officers (ATSCOs), as required (exhibit 1C).

c. Issue command security procedures for offices under their cognizance.

4. Requests for Investigative Assistance

a. DNS-34, liaises with the Naval Criminal Investigative Service (NCIS), Office of Personnel Management (OPM), Defense Security Services (DSS) and PFPA on matters of PSIs and civil or criminal investigative. OPNAV security officers and coordinators will report all incidents of actual, suspected or alleged criminal offenses to DNS-34 upon discovery.

b. Investigation, or other action as appropriate, will be initiated within 24 hours to ensure expeditious resolution while protecting national interests and individual’s due process.

5. Counterintelligence (CI) Matters: will be reported to NCIS for appropriate action. All OPNAV security serviced activities’ personnel, whether they have access to classified information or

not, will report to DNS-34 any activities involving themselves, their dependents or others. DNS-34 will, in turn, notify NCIS.

6. Foreign Travel: reported in advance to DNS-34. For Out of Continental United States (OCONUS) travel, personnel will attend foreign travel briefing within 12 months.

7. Emergency Plan Procedures.

a. The Navy Continuity of Operations Plan, reference (j), discusses essential requirements for continuity of operations during war/emergency situations. Essential records not pre-positioned may be hand-carried in accordance with references (b), volume 3, and (d).

b. In case of evacuation due to fire or natural disaster, individuals in open storage vaults will evacuate and lock the combination lock on door (do not set the alarm). Place classified information in security containers and lock it as long as there is no threat to personal safety. PFPA will provide perimeter protection of areas involved.

8. Security Education, Training and Awareness (SETA): Will be administered in accordance with references (b) and (c) and as aligned to DON training and awareness policy at, http://www.secnav.navy.mil/dusnp/Security/Pages/Default.aspx.

9. Debriefings

a. Required prior to termination of active military service or civilian employment including temporary separation for a period of 60 days or more, including sabbaticals and leave without pay.

b. When security clearance is revoked.

c. An OPNAV 5511/14 Security Termination Statement will also be executed when a member inadvertently gain access to classified information.

10. Waivers

a. When OPNAV security serviced activities can’t met this instruction mandates, waiver requests will be forwarded to DUSN(P)/SD per reference (c).

11. Information Management Control and Forms

a. Information Management Control

(1) Reporting requirements contained in chapter 1 (paragraphs 4, 5 and 6), chapter 2 (paragraph 4a) , chapter 12 (paragraph 6h) and chapter 15 (paragraphs 1a,1b,1d,1e and 2) of this manual are exempt from reports control per SECNAV M-5214.1 of December 2005, part IV, subparagraphs 7c, 7g , 7k and 7n.

(2) Reporting requirement contained in chapter 15 (paragraph 1c) of this manual is assigned to OPNAV RCS 5510-6C.

b. Forms. See Appendix (C) of this manual for applicable forms.

Exhibit 1A

5510
Date

From: Directorate Head
To: Individual Appointed (full name, office code, Location and telephone number)

Subj: DESIGNATION AS COMMAND SECURITY COORDINATOR

Ref: (a) OPNAVINST 5510.60N
(b) OPNAV 5510.1
(c) SECNAV M-5510.36 of June 2006
(d) SECNAV M-5510.30 of June 2006

1. Per reference (a) and (b), you are appointed as Command Security Coordinator. Your initial period of appointment will be from _____ until _____. You will be notified in writing of any change in this appointment.

2. You are directed to become thoroughly familiar with references (b) through (d) as applied to your specific organization. Along with the OPNAV Security Manager (DNS-34), you are to make certain that security policies are effectively implemented in a cohesive manner. You will ensure that all personnel, especially those assigned special security responsibilities, are advised of any security policy changes.

3. For effective management of the program, you must:

a. Serve as the head advisor and direct representative of the directorate head in matters pertaining to security, and serve as the communication link between DNS-34 and command personnel.

b. Develop written security procedures, including an emergency plan. These procedures will be consistent with reference (a) with specifics and coverage for those items listed in chapter 1, section 3(d).

c. Coordinate and implement the security education program.

d. Ensure that threats to security, compromise and other security violations are promptly reported, recorded and, when

SAMPLE

necessary, vigorously investigated. Monitor existing security control systems (document, physical, etc.) for effective operation.

e. Administer the program for classification, declassification and downgrading of classified information.

f. Ensure compliance with accounting and control requirements for classified material, including receipt, distribution, inventory, reproduction and disposition.

g. Formulate and coordinate physical security measures for protection of classified materials.

h. Ensure security control of classified visits to include outgoing visit requests via Joint Personnel Adjudication System (JPAS).

i. Ensure protection of classified information during unclassified visits.

j. Ensure, where applicable, compliance with the Industrial Security Program for classified contracts with DoD contractors.

k. Ensure that all personnel who are to handle classified information or to be assigned to other sensitive duties, are appropriately cleared, and that requests for security clearances are properly prepared, submitted and monitored.

l. Ensure that access to directorate classified information is limited to those with a "need to know."

m. Coordinate program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

n. Ensure that appropriate security briefings and debriefings are scheduled and given to each individual departing on or returning from foreign travel.

o. Ensure that required briefings are provided to personnel before attending meetings anywhere it can be anticipated that foreign representatives will participate.

p. Ensure that every required precaution is taken to prevent unauthorized disclosure when individuals are hand-carrying classified material within the command in the

SAMPLE

performance of daily duties, or outside the command in a travel status.

q. Ensure that adequate security measures are provided in advance, during, and after meetings or conferences, to include seminars, exhibits, symposiums, conventions, training activities, workshops, or other such gatherings, where classified information will be disseminated.

r. Evaluate the effectiveness of the Security Program by conducting annual division security inspections using the Annual Self-inspection Program Data Report checklist identified at reference (b) volume 1, enclosure (2).

s. Assist DNS-34 in the identification of potential problems affecting the Security Program and report such items to DNS-34.

t. Assist DNS-34 with other security duties as required.

u. Perform those duties assigned to Assistant Security Coordinators in their absence.

4. You are the Command Security Coordinator. Your signature below acknowledges your responsibility for this program. Your support and professionalism are necessary for success, and while each person, military, civilian and contractor, are individually responsible for our national security through compliance with security regulations, your leadership in this program ensures that security.

Designee's Signature:_____

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (DNS-34)

SAMPLE

EXHIBIT 1B

5510
date

From: Directorate Head
To: Individual Appointed (full name, office code, Location and telephone Number)

Subj: DESIGNATION AS COMMAND ASSISTANT SECURITY COORDINATOR

Ref: (a) OPNAVINST 5510.60N
(b) SECNAV M-5510.36 of June 2006
(c) SECNAV M-5510.30 of June 2006

1. Per reference (a), you are appointed as the office code Assistant Security Coordinator for _____. Your initial period of appointment will be from _____ until _____. You will be notified in writing of any change in this appointment.

2. For effective management of the program, you must:

(a) Serve as a communication link between the Security Coordinator and cognizance staff personnel.

(b) Report security violations to the Security Coordinator.

(c) Ensure that personnel under your cognizance conform to the guidance of references (a), (b), and (c) and report discrepancies to the Security Coordinator and the immediate supervisor.

(d) Relay problems or items requiring clarification to Security Coordinator.

(e) Assist the Security Coordinator with other security duties as required.

3. I request your support and professionalism in helping to carry out this vital program. At the forefront of the thoughts of all directorate personnel should be that each person,

SAMPLE

military or civilian, in this command is individually responsible for our national security through compliance with security regulations.

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (DNS-34)

SAMPLE

EXHIBIT 1C

5510
Date

From: Directorate Head
To: Individual Appointed (full name, office code, location and telephone number)

Subj: DESIGNATION AS TOP SECRET CONTROL OFFICER

Ref: (a) OPNAVINST 5510.60N
(b) OPNAV M- 5510.1
(c) SECNAV M-5510.36 of June 2006

1. Per reference (a), you are appointed as Directorate Top Secret Control Officer. Your period of appointment will be for at least 1 year, from _____ until _____. You will be notified of any change in this appointment.

2. You are directed to become thoroughly familiar with references (a) through (c) as they apply to your specific organization. Along with the Directorate Security Coordinator and the OPNAV Security Manager (DNS-34), you are to make certain that security policies applicable to Top Secret material are effectively implemented in a cohesive manner. You will ensure that all personnel with Top Secret access, especially those assigned Top Secret control responsibilities, are advised of any security policy changes.

3. For effective management of the program, you must:

a. Serve as the head advisor and direct representative of the directorate head in matters pertaining to Top Secret control, and serve as the communication link between the OPNAV Security Manager (DNS-34) and command personnel.

b. Develop written Top Secret control procedures to be included in the command's security procedures. These procedures should be consistent with references (a) through (c).

SAMPLE

c. Administer program for classification, declassification and downgrading of Top Secret information.

d. Ensure compliance with accounting and control requirements for Top Secret material, including receipt, distribution, inventory, reproduction and disposition.

e. Ensure that all personnel who are to handle Top Secret information are appropriately cleared.

f. Conduct the annual inventory required by reference (a).

g. Ensure that access to Top Secret information is limited to those with a "need to know" and records of disclosure are properly executed.

h. Evaluate the effectiveness of the Top Secret Control Program by conducting annual division security inspections per exhibit 2C of reference (c).

i. Perform those duties assigned to assistant Top Secret Control Officers in their absence.

4. You are the Directorate Top Secret Control Officer. Your signature below acknowledges your responsibility for this program. Your support and professionalism are necessary for success, and while each person, military, civilian and contractor, are individually responsible for our national security through compliance with security regulations, your leadership in this program ensures that security.

Designee's signature: _____

Signature of Directorate Head

Copy to:
Personnel File
OPNAV Security Manager (DNS-34)

SAMPLE

CHAPTER 2
PERSONNEL SECURITY

1. Basic Policy

a. Security access to classified information or assignment to sensitive duties will be granted only after a favorable personnel security determination, and execution an SF 312 Classified Information Nondisclosure Agreement. Initial determination will be based on a Personnel Security Investigation (PSI) appropriate to the access level required.

b. Access will not be granted to members who possess a foreign passport. Member will be directed to return the passport to the appropriate country embassy or consulate, requesting a return receipt to document the passport was surrendered. As an alternative, member may elect to destroy the passport in presence of security official. In addition, dual citizens will provide a signed statement expressing their willingness to renounce dual citizenship.

c. U.S. citizenship is requirement for personnel occupying DON sensitive and information technology (IT) positions. IT access categories are based on the level of information system (IS)/network access required for responsibilities of the position and the associated potential for adverse impact on the DoD mission. OPNAV Security (DNS-34) will designate each sensitive position as requiring privileged, limited privilege, or non-privileged access in accordance with reference (c).

d. Title 10, United States Code (U.S.C.), precludes the initial granting or renewal of security clearance by DON personnel under circumstances outlined by “Smith Amendment.”

(1) Conviction with imprisonment exceeding 1 year;

(2) Unlawful user, addicted to, a controlled substance;

(3) Mentally incompetent, determined by a mental health professional; or

(4) Discharged or dismissed from the Armed Forces under dishonorable conditions.

e. Final determinations are by Department of Defense Consolidated Adjudication Facility (DODCAF) however SECNAV may authorize a meritorious waiver of the prohibitions.

f. Personnel requiring a PSI will use Office of Personnel Management (OPM) Electronic Questionnaires for Investigations Processing (E-QIP) to submit the investigation. To gain access to the OPM E-QIP web site, notification will be provided by DNS-34B. Once notified, member will have 30 calendar days to access the OPM web site to begin the PSI or access will be terminated. Reinstatement of access will be granted either by DNS-34, as required, following either a phone call or e-mail notification. Before accessing the E-QIP web site, the member should review the Applicant's E-QIP Handbook located at http://www.opm.gov/investigations/e-qip-application/completingsf86.pdf under E-QIP latest updates.

h. Fingerprinting: Fingerprints will be taken electronically. The prints will be printed out on SF 87 Finger Print Chart and either provided to the requesting member or forwarded electronically to OPM for processing with the appropriate security investigation request.

i. PSI upgrade requests will require a valid billet assignment, justification letter signed by an O-6 or above, and a new OPNAV 5510/418 Security Indoctrination Certification and Request for Clearance and Special Accesses.

2. Request for Clearance Eligibility and Access

a. All civilian and military personnel reporting aboard OPNAV security serviced activities are required to check-in with DNS-34 with an OPNAV 5510/418 completed by the Security Coordinator or Assistant Security Coordinator.

b. Security Coordinators will complete the OPNAV 5510/418 requesting the required level of access needed for the billet, and member will read and sign the "Security Awareness Briefing Objectives" statement on back of the form.

c. DNS-34B will document clearance eligibility ensuring member has an in-scope investigation required for the access requested. If the individual's investigation is out of scope, DNS-34B will take action to arrange for initial investigation or periodic reinvestigation, as applicable via E-QIP.

d. Until the Security Coordinator has received notification from DNS-34B that an individual's clearance eligibility/access has been granted, access to classified information is not authorized.

e. When a final clearance eligibility has been granted by DODCAF, the information will post in JPAS, and DNS-34B will update member's JPAS record to reflect final clearance eligibility and "United States" access.

f. Special one-time access to a level higher than that for which they are eligible may be granted in accordance with reference (d).

g. Reference (d) also allows for Emergency Appointment to sensitive positions for civilian personnel after a statement that a check of locally available records was favorable and coordinated with Human Resource (HR) and the command's Security Coordinator.

3. Classified Information Nondisclosure Agreement, SF 312 is to be executed by all cleared Government and non-government personnel as a condition of access to classified information. Refusal to execute the SF 312 will be grounds for denial of access to classified information.

4. Continuous Evaluation of Eligibility

a. Any person having knowledge or information reflecting on an individual's loyalty, reliability and trustworthiness from a security perspective will immediately report the full particulars and circumstances to DNS-34 for evaluation and/or further reporting.

b. Self-reporting requirements are implemented per reference (d). Supervisors and co-workers are cautioned that information which could place an individual's loyalty, reliability and trustworthiness in question has to be evaluated from a security perspective

5. Administrative Withdrawal or Adjustment of Clearance

a. When a clearance is administratively withdrawn, the individual will be debriefed in accordance with paragraph 4-11 of reference (d).

b. Administrative withdrawals or lowering of security clearance access is not authorized for cause (i.e., when disqualifying information about the individual is known).

c. When security clearance access is administratively withdrawn or lowered, DNS-34B will update JPAS to show action was taken administratively and without prejudice to the individual.

6. Denial or Revocation and Suspension of Clearance/Access for Cause as described in chapter 8 of reference (d).

7. Access to Critical Nuclear Weapon Design Information (CNWDI)

a. Because of the extreme sensitivity of CNWDI, access to and dissemination of CNWDI information must be limited, as outlined by Reference (j), to the minimum number of persons requiring access in performance of their official duties. Security policy guidance will be strictly observed with special administrative controls established at exhibits 2C through 2F to outline procedures and to positively identify those personnel requiring access to CNWDI.

b. OPNAV security serviced activities outlined at exhibit 2G will implement the procedures outlined in exhibits 2C through 2F for those personnel under their cognizance requiring access to CNWDI.

EXHIBIT 2A

5520
Date

MEMORANDUM FOR OPNAV SECURITY BRANCH (DNS-34)

Subj: EMERGENCY APPOINTMENT TO A NONCRITICAL SENSITIVE POSITION

Ref: (a) OPNAVINST 5510.60N
(b) SECNAV M-5510.30 of June 2006

Encl: (1) Security Indoctrination Certification and Request for Clearance

1. Per reference (a), the following emergency appointment is submitted for the below named incumbent whose position is designated non-critical sensitive:

Full Name: DOB: POB:
SSN: Position/Job Title:

2. A National Agency Check and Inquiry/National Agency Check on (Name),(Grade), was submitted to the Office of Personnel Management/Defense Investigative Service on (Date) and local records check was favorable. A request for security access is submitted as enclosure (1). Request an Interim Secret clearance be granted per reference (b).

3. This exception is necessary because the delay in appointment incurred while awaiting final completion of the investigative requirements would be harmful to the national interest because (state the reason why).

4. Mr./Mrs./Miss/Ms. (Name), (OPNAV NCode/Navy Staff Office) will be advised to read and thoroughly familiarize himself/herself with references (a) and (b) in order to properly perform his/her assigned duties.

5. It is understood that Interim Secret clearance is automatically cancelled 6 months from the date granted, upon granting final access, or upon transfer to duty outside (your division).

Copy to:

SAMPLE

Cognizant Security Coordinator
Cognizant HRD

SAMPLE

EXHIBIT 2B

5520
Date

MEMORANDUM FOR OPNAV SECURITY BRANCH (DNS-34)

Subj: EMERGENCY APPOINTMENT TO A CRITICAL SENSITIVE POSITION

Ref: (a) SECNAV M-5510.36
(b) OPNAVINST 5510.60N

Encl: (1) Security Indoctrination Certification and Request for Clearance (OPNAV 5510/418)

1. Per reference (a), the following emergency appointment is submitted for the below named incumbent whose position is designated critical sensitive:

Full Name: DOB: POB:
SSN: Position/Job Title:

2. A Background Investigation/Special Background Investigation on (Name), (Grade), was requested on (Date). A satisfactory NACLC/ANACI was completed on (Date) by the Office of Personnel Management/Civil Service Commission/Defense Investigative Service. A request for security access is submitted as enclosure (1). It is requested that an interim Top Secret clearance be granted per reference (b).

3. This exception is necessary because the delay in appointment incurred while awaiting final completion of the investigative requirements would be harmful to the national interest because (state the reason why).

4. Mr./Mrs./Miss/Ms. (Name), (OPNAV NCode/Navy Staff Office) will be advised to read and thoroughly familiarize himself/herself with references (a) and (b) in order to properly perform his/her assigned duties.

5. It is understood that Interim Top Secret clearance is automatically cancelled 6 months from the date granted, upon granting final access, or upon transfer to duty outside (your division).

Copy to:

SAMPLE

Cognizant Security Coordinator
Cognizant HRD

SAMPLE

EXHIBIT 2C

PROCEDURES FOR CERTIFYING ACCESS TO CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION (CNWDI)

1. Screening Procedures. Prior to certifying an individual for access to CNWDI, the following prerequisites must be verified:

a. The prospective recipient must have a valid DoD security clearance (final Top Secret or Secret) based on the appropriate investigative requirements.

b. The prospective recipient must require access to nuclear weapons design information in the performance of his/her official duties. Strict adherence to the "need to know" principle must be observed.

2. Certification Procedures. The following procedures are to be followed when certifying an individual for access to CNWDI:

a. Verify the basic prerequisites outlined in paragraph 1 above.

b. Execute the interoffice memo outlined in exhibit 2E, ensuring that the appropriate certifying officials (at exhibit 2G) sign the document. Document may also be signed as "for," "by direction," or "acting," as appropriate, in the absence of the certifying official.

3. Update Procedures

a. Additions. Conduct screening, certification and submit interoffice memo in accordance with paragraphs 1 and 2 above.

b. Deletions. Provide copy of signed Debriefing Certificate to DNS-34.

SAMPLE

EXHIBIT 2D

BRIEFING/DEBRIEFING CERTIFICATE

CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION

PART I

1. I acknowledge that I have been authorized to receive or hold Critical Nuclear Weapons Design Information. I understand that the security of Critical Nuclear Weapons Design Information is of paramount importance and that unauthorized disclosure of such information will endanger the United States.

2. I understand that when I have a change in my assignment or duty which makes it no longer necessary for me to have access to Critical Nuclear Weapons Design Information, I must execute a Debriefing Certificate.

3. I am aware that I am subject to penalties under the Atomic Energy Act of 1954, the United States Espionage Laws, or the U.S. Code, Title 18, if I discuss with, or disclose Critical Nuclear Weapons Design Information to any person not currently authorized to have such information.

(Date) (Signature)
(Signature of Witness) (Name Printed or Typed)

PART II

1. I acknowledge that I am no longer authorized access to Critical Nuclear Weapons Design Information. I certify that, hereafter, I will not divulge or discuss such information which I have acquired as an authorized recipient, unless required to do so by a competent authority.

2. I am aware that I am subject to penalties under the Atomic Energy Act of 1954, the United States Espionage Laws, or the U.S. Code, Title 18, for any unauthorized disclosure.

(Date) (Signature)
(Signature of Witness) (Name Printed or Typed)

SAMPLE

EXHIBIT 2E

5210
Date

From: (OPNAV Security Serviced Activity)
To: OPNAV Security (DNS-34)

Subj: CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION, CERTIFICATION OF NEED-TO-KNOW

Ref: (a) DoD Instruction 5210.2
(b) OPNAVINST 5510.60N

Encl: (1) Personnel certified for access to Critical Nuclear Weapons Design Information

1. Per references (a) and (b), the personnel listed in enclosure (1) are certified as having a "need to know" for Critical Nuclear Weapons Design Information (CNWDI).

2. Briefing certificate(s) has/have been completed.

(Signed by Certifying Official)

SAMPLE

EXHIBIT 2F

PERSONNEL CERTIFIED FOR ACCESS TO
CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION

FOUO - This record contains information subject to the provisions of the Privacy Act (P.L. 93-579). This personal data is intended for the use in a confidential manner for security purposes.

FULL NAME SSN	RANK/RATE OR GRADE	OFFICE CODE & BILLET TITLE	CERTIFICATION & EXPIRATION DATE

SAMPLE

EXHIBIT 2G

List of OPNAV Security Serviced Activities CNWDI Certifying Official

Secretary of the Navy
Under Secretary of the Navy
Assistant Secretary of the Navy
(Research, Development & Acquisition)
Assistant Secretary of the Navy
(Manpower & Reserve Affairs)
Administrative Aide to the Secretary of the Navy
Director, Office of Program Appraisal
Chief of Naval Operations (N00)
Vice Chief of Naval Operations (N09)
Director Navy Staff (DNS)
Director of Naval Information Dominance (N2/N6)
Deputy Chief of Naval Operations
(Manpower, Personnel, Training & Education) (N1)
Deputy Chief of Naval Operations
(Plans, Policy & Operations) (N3/N5)
Deputy Chief of Naval Operations
(Fleet Readiness & Logistics) (N4)
Director, Supply, Ordnance, & Logistics Operations Division
(N46)
Deputy Chief of Naval Operations
(Integration of Capabilities & Resources) (N8)
Director of Navy Test & Evaluation & Technology Requirements
(N84)
Director, Test & Evaluation Division (N842)
Deputy Chief of Naval Operations
(Warfare Systems) (N9)
Surface Warfare Branch (N96)
Submarine Warfare Branch (N97)
Air Warfare Branch (N98)

SAMPLE

CHAPTER 3
CONTROL ACCESS CARD (CAC) ISSUANCE, PROPERTY PASSES, AND TRUSTED ASSOCIATE SPONSORSHIP SYSTEM (TASS)

1. DoD Building Access

a. Background. The Washington Headquarters Services (WHS), Physical Security Division is responsible for setting policies for issuance of DoD building access in accordance with reference (l).

b. Building access will be issued minimally for one month and not to exceed the date as established by the members' CAC or expiration date of last investigation. Each individual must show his/her CAC to police officer upon entering the Pentagon. The DoD CAC must be displayed visibly on outer clothing at all times. CAC holders must exercise proper precautions to prevent loss of their card. In the event a CAC is lost, it must be reported immediately to the Security Manager and Pentagon Building Pass Office. The Pentagon Building Pass Office will replace the CAC upon receipt of memorandum from the DNS-34 and a signed DD 2249 DoD Building Pass Application.

c. A favorably adjudicated investigation is required for issuance of permanent building CAC access. Temporary access will be issued upon completion of National Criminal Investigation Check (NCIC) to new members upon arrival to allow for completion of E-QIP investigation requirements. Advance coordination is required between HR and DNS-34 due to the processing lead time of 3 to 5 days for NCIC.

2. Property Passes

a. The removal of property from the Pentagon and other DoD locations is governed by WHS, Physical Security Division, and PFPA. Reference (l) requires that the authorized removal of Government property not covered by a bill of lading or invoice must be accomplished by an OF 7 Property Pass, or memorandum on official business letterhead including description of the property and date of issue.

b. The property pass or memorandum will be given to PFPA officers when exiting the building.

3. Trusted Associate Sponsorship System (TASS). Sponsored by the Defense Manpower Data Center (DMDC), as directed by Homeland Security Presidential Directive-12, is an automated process to

authorize the issue of a CAC to DoD contractors.

a. TASS is a Web-based application that receives automatic personnel data from the Defense Enrollment and Eligibility Reporting System (DEERS), eliminating paperwork for issuance of CAC to contractors.

b. Electronic applications are processed, reviewed and stored by delegated Trusted Agents (TAs) at the command level.

c. OPNAV security serviced activities are responsible for appointment of a TA, which can be concurrently staffed by the command's Security Coordinator.

d. OPNAV Security Branch personnel DNS-34/34D will serve as the TA Security Manager under the TASS.

e. TAs will initiate contractor's CAC request in the system.

f. Contractors must have submitted information required for the issuance of a CAC using the TASS Web application. The application will not be processed until it has been submitted in complete format.

g. Completed application is submitted with system automatically notifying the TA.

(1) TA then logs into TASS to review, approve or reject the application.

(2) If approved, the system will automatically update DEERS with the contractor's information and direct the contractor via e-mail to proceed to a Real-Time Automatic Personnel Identification System (RAPIDS) workstation for CAC issuance.

(3) If rejected, the system notifies the contractor.

h. Contractor's CACs are revalidated every 6 months by TAs upon automatic system notifications or as initiated by the DMDC.

CHAPTER 4
CLASSIFICATION

1. Basic Policy

a. Reference (a) is the basis for classifying national security information except as provided in the Atomic Energy Act of 1954, as amended. Classification management and authority for DoD activities are provided at reference (b), volume I, enclosure (4). DON classification management is delineated in reference (c) including mandated training for Original Classification Authorities (OCAs) and derivative classifiers.

b. Ultimate authority for information classification across OPNAV commands resides with the OCAs as exercised via assigned Subject Matter Experts (SMEs). OPNAV Security Coordinators and the Security Manager have vital roles with implementation, documentation and reporting of decisions as well as staffing and promulgation of required program Security Classification Guides (SCGs). Final inherent responsibilities remain with each individual holder of information which warrants safeguarding, therefore all assigned members must be reminded of contracted obligation under the classified non-disclosure agreement (SF 312).

2. Cover Sheets and Classification Labels

a. Cover sheets are required when hand carrying of such materials within inner building passageways and corridors. reference (b), volume 2, enclosure (2), provide specific requirements for attaching the appropriate classified document cover sheet (Standard Form (SF) 703, “Top Secret (Cover sheet);” SF 704, “Secret (Cover sheet);” or SF 705 “Confidential (Cover sheet)”) to classified once moved from storage.

b. To meet this requirement for electronic media, the SF 706, (“Top Secret”), SF 707, (“Secret”) and SF 708, (“Confidential”), SF classification labels must be used to identify the highest level of classified information stored on IT systems and removable electronic storage devices

3. Classification Designations.

Information that requires protection against unauthorized disclosure in the interest of national security must be classified as Top Secret, Secret, or Confidential, as denoted in references (a) through (d).

4. For Official Use Only (FOUO)

a. FOUO, a subcategory of CUI, applies to information which requiring protection under the criteria of an reference (a), and which contain information which may be withheld from the public per reference (m). No other material must be considered or marked FOUO, as FOUO is not authorized as a form of classification to protect national security interests.

b. For CUI and FOUO marking and safeguard requirements, refer to reference (b), Volume 4. Use DD Form 2923 to protect individual's personal information.

5. Original Classification Authority

a. The authority to originally classify information as Top Secret, Secret or Confidential is granted by SECNAV to DON officials as established by reference (b), Volume 1 and reference (c).

b. DON incumbent positions, identified by DUSN (P) at reference (c), aren't delegable. If an OCA is absent, however, the person designated to act in his/her absence may exercise the classification authority.

c. DNS-34 will coordinate with OPNAV security serviced activities to ensure designated OCA officials are trained annually on their classification responsibilities. All original classification authorities must be indoctrinated in the fundamentals of security classification, limitations of their authority to classify and their responsibilities.

d. OPNAV designated OCAs will maintain an accurate list of classification decisions for annually reporting via DNS-34 to DUSN (P)/SD via SF 311 Agency Security Classification Management Program Data, per reference (b), Volume 1.

6. Original and Derivative Classification.

a. Original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure and a determination of the level of protection required. Detailed original classification and program protection determinations are issued as part of the program SCG as indicated below.

b. Derivative classification is accomplished by anyone who incorporates, paraphrases, restates, or generates, in new form,

information which is already classified. All OPNAV members with classified access, SIPRNET accounts, and classified document access are derivative classifiers and will:

(1) Comply with requirements contained in reference (b) including receipt of biennial training.

(2) Mark email and TOP SECRET information as final documents at origin.

7. Security Classification Guide (SCG)

a. SCGs are recordings of DON original classification determinations for security management and program use. SCGs serve as the primary source reference for derivative classifiers to identify the level and duration of classification for a specific program element.

b. DON OCAs will prepare SCGs for each DON system, plan, program, or project under their cognizance in the format described reference (m).

c. OCAs must review their SCGs for accuracy and completeness at least every 5 years.

CHAPTER 5
MARKING

1. Basic Policy

a. OPNAV security serviced activities will adhere to the marking principles of reference (b), volume 2 (enclosures 3 and 4), and reference (c), chapter 2.

b. When re-generating, paraphrasing or reproducing classified materials ensure that classification markings are carried forwarded with particular attention to include the derivative classifier in the signature authority block; to mark portion (including subjects) to the left of text; and to include a list of source documents when denoting "multiple sources" as "classified by".

c. All classified must be marked in a manner that leaves no doubt about the level of classification assigned.

2. Marking Classified Documents and Correspondence

a. All classified documents and correspondence will be personally reviewed by Command Security Coordinator who will coordinate with OPNAV Security Manager prior to approval.

b. Classified productions such as directives, instructions, and tasks will be populated in TV-5 SIPRNET for official Security Coordinator and DNS-34 review and endorsements prior to clearance for final signature and production.

c. Marking of CUI and FOUO materials will be done in accordance with reference (b) volume 4.

d. Classified e-mails will be marked as finished documents.

e. Top Secret working papers will be marked and accountable as finished product.

CHAPTER 6
HAND CARRYING OF CLASSIFIED MATERIAL

1. Within a Command or Immediate Environs

a. Classified material carried within the OPNAV security serviced activities or immediate environs will include cover-sheet, identified chapter 4, paragraph 2, over the material to prevent inadvertent disclosure.

b. When movement requires transportation other than walking, double-wrap and address the classified material with classification stamped on inside wrapping. Specific wrapping, addressing and receipt instructions are located at chapter 10.

c. Contractor personnel are authorized to hand carry classified material from OPNAV security serviced activities spaces with prior arrangements and approval of DNS-34. Request to hand carry classified material must meet the requirements outlined in chapter 13, paragraph 3 of this manual. A valid visit request and courier authorization must be on file with clearance and access verified in JPAS.

2. Travel Authorization to Hand Carry Classified Material

a. Requires DNS-34 approval and individual designated as courier must possess a DoD or contractor-issued identification card and a government-issued photo identification card.

b. The courier will have a DD 2501 Courier Authorization (courier card) and execute the "Classified Courier Responsibility Acknowledgment" (exhibit 6A).

c. Provide DNS-34 an original letter on letterhead stationary authorizing hand carry of the material, prepared for DNS-34 signature prior to travel (exhibit 6B).

3. Procedures for Carrying Classified Documents Aboard Commercial Passenger Aircraft are delineated at reference (b), volume 3, enclosure 4.

a. Traveler carrying classified documents aboard a commercial aircraft will proceed through airline ticketing and boarding procedures in the same manner as other passengers.

b. While traveling:

(1) The traveler must make sure the classified documents being carried have no metal bindings and are in double, sealed envelopes.

(2) The traveler must present his/herself at the screening station for routine processing.

(3) Upon arrival at the screening checkpoint, courier must ask to speak to the Transportation Security Agent (TSA) Supervisory or Transportation Security Officer and present the required identification and authorization documents including valid courier authorization, DoD or contractor-issued identification card, and government-issued photo identification card. TSA officials may still require the classified material to be screened in accordance with their standard procedures.

(4) When the TSA authority confirms the courier's authorization to carry classified material, the courier and all of the courier's personal property must be provided for screening. The classified material must remain within the courier's sight at all times during the screening process. The screening official may be able to inspect the envelopes by flexing, feel, weight, etc., usually without requirement for opening the envelopes themselves.

(5) The screening official may process the envelopes with a detection device. If no alarm results, the envelopes require no further examination. If an alarm sounds, make arrangements with the security official to open the package out of sight of the general public. Contact the OPNAV Security Operations Center, (703) 697-3454 or 697-1310) during normal hours of 0700-1600, and the Navy Operational Center, (703) 695-0231 after normal business hours.

4. Procedures for Courier Authorization Cards

a. DD 2501 Courier Authorization Cards are for use by individuals hand carrying classified material out of assigned buildings by means of surface transportation within a commuting area of the command. Security Coordinators will submit requests for DD 2501s to DNS-34 via memorandum or e-mail. The request must include: name, rank, SSN (last four), and clearance level requested.

b. DNS-34 will review all requests for DD 2501s and issue cards as justified. The form is issued for no more than 2 years. The requirement for authorization to hand-carry

classified information must be reevaluated and/or revalidated at least once every 2 years.

c. DD 2501s will be released to either the Security Coordinator or the individual courier.

d. Security coordinators are responsible for maintaining accountability and control of DD 2501s issued under their cognizance to include retrieval of the cards when members detach from the command.

e. DD 2501s will be issued to individuals strictly on an "as needed" basis and must be returned to the Security Coordinator upon permanently departing the command.

EXHIBIT 6A

CLASSIFIED COURIERS RESPONSIBILITY ACKNOWLEDGMENT

The following is a list of responsibilities under DODM 5200.01 which apply to all authorized couriers of classified material:

1. Classified material must be in my physical possession at all times, unless under proper storage at a United States Government activity or an appropriately cleared contractor facility.

2. If necessary, overnight storage has been arranged with a Government activity or cleared contractor facility.

3. I will retain a receipt, signed by an authorized representative of the Government activity or contractor facility, upon surrendering classified material for overnight storage.

4. When classified material is carried in a private, public or government conveyance, I will not store it in any detachable storage compartments, such as automobile luggage racks, aircraft travel pods or drop tanks.

5. I may not read, study, display or use classified material in any manner on a public conveyance or in a public place.

6. A complete detailed list of the contents of the material to be transported has been left with a designated authority in my activity.

7. I understand that there is no assurance of immunity from search by security, police, customs, and/or immigration officials on domestic or international fights. If necessary, it may be opened out of sight of the general public.

I have read, fully acknowledge and understand my responsibilities as an authorized courier of classified material.

_____ _____

(DATE) (SIGNATURE)

SAMPLE

EXHIBIT 6B

Date of issue

From: Chief of Naval Operations
To: To Whom It May Concern
Subj: COURIER AUTHORIZATION

1. Mr. John Thomas Doe (full name) of Chief of Naval Operations (name of activity) is authorized to hand carry three sealed packages, 9" X 8" x 24" (describe package(s) being carried) from Chief of Naval Operations, Pentagon, Washington, DC (addresser) to U.S. Naval Postgraduate School, Monterey, CA (addressee name) on 14 June 2014 (date)

2. Flight #XX departs (Insert Name) Airport at XXXX and arrives at (insert flight information including transfer points) (Insert Name) Airport at XXXX.

3. Mr. John Doe (name of courier) will carry a DoD Badge #12345 (type of I.D. w/photo.) (If the courier is a civilian, include height, weight, date of birth and signature.)

4. This authorization expires 0900/07 June 1989 (Time/date not to exceed 7 days from date of issue.)

5. Confirmation of this authorization may be obtained by calling (703) 697-3454 or DSN 227-3454, M-F, 0700-1700, or (703) 695-0231, during abnormal hours, weekends and holidays.

6. This package contains classified material and is not to be opened in the general public under any circumstances. If it is necessary for the package to be opened and inspected, it is requested that the security agency assist with securing the package to the original state and sign the package after it is secured.

ALPHONSO W. MOORE
Director, Security Programs/
Command Security Manager

Copy to:
DNS-34

SAMPLE

CHAPTER 7
ACCOUNTING AND CONTROL

1. Basic Policy

Classified information must be afforded a level of accounting and control commensurate with its assigned classification. OPNAV accounting and control measures will be implemented to cover receipt and handling, limit dissemination, prevent unnecessary reproduction, and address disposition requirements specified by references (a), (b) and (c). Particular attention will be afforded to preventive measures precluding damages to national security which might result from unauthorized disclosure of classified information.

2. Top Secret

a. OPNAV security serviced activities anticipating handling or receipt of Top Secret documents or material will designate a TSCO in accordance with Exhibit 1C. The designated TSCO is responsible for receiving, maintaining accountability, distributing, reproducing and the destruction of all Top Secret material as outlined by volume 3, reference (b). Minimum requirements include establishment of accountability register, Serializing of copies, and maintenance of "Record of Page Checks."

b. Top Secret documents will be physically sighted, or accounted for by examination of written evidence of proper disposition, such as certificate of destruction, transfer receipt, etc., at least once annually, change of TSCO, and more frequently when circumstances warrant. At the same time, the TSCO will audit Top Secret records to determine completeness and accuracy. Procedures for conducting the Top Secret audit and inventory are located at exhibits 7A and 7B. Findings are reported as outlined at exhibit 7C.

c. Retention of Top Secret documents will be kept to a minimum. Return Top Secret documents to the TSCO for destruction as soon as their intended purpose has been served. When Top Secret is destroyed, prepare a record of destruction identifying the material destroyed, the date destroyed, and the two officials who witnessed its destruction.

d. Account for Top Secret material by a continuous chain of receipts. Hand-to-hand transfer with signed receipts is required for internal distribution of Top Secret, with a record

kept of each individual to whom the information is disclosed through use of OPNAV 5511/13 Disclosure Record.

e. Top Secret material will only be reproduced by the TSCO and may not be reproduced without the consent of the originating agency or higher authority. Authority to reproduce will be obtained by the individual requiring the reproduction and forwarded with the Top Secret document to their TSCO for action.

3. Secret

a. Within the OPNAV security serviced activity, administrative security procedures will be established for controlling Secret material to include: (1) originated or received by the command; (2) distributed or routed to divisions or branches within the command; and (3) disposition.

b. Receipts are only required when Secret material accountability will be transferred from one command to another.

c. Transport or ship Secret material by U.S. Postal Service (USPS) registered mail within and between the United States and its territories, or use of overnight domestic express delivery as delineated in reference (b). When mailing Secret material, enclose a receipt identifying the document(s). When receiving, receipt must be signed and returned to the sender within 3 days of receipt. The sender cannot be sure that accountability has been transferred until the recipient signs and returns the receipt.

d. To safeguard messages and protect them appropriately to their level of classification, control internal routing through "need to know" and reproduce Secret messages only per the requirements outlined in chapter 8, paragraph 1, of this instruction.

e. Refer to chapter 10 of this instruction for transmission of Secret classified materials via approved communications circuits.

4. Confidential. There is no requirement to maintain records of receipt, distribution, or disposition of OPNAV Confidential material. Administrative provisions are required, however, to protect Confidential information from unauthorized disclosure and compliance with the regulations on marking, storage, transmission and destruction.

5. Secret and Confidential Working Papers

a. Working papers are documents and materials accumulated or created in preparation of finished documents and materials. Working papers must be:

(1) Dated when created;

(2) Conspicuously marked, centered top and bottom of each page with the highest overall classification level of any information they contain, along with the words "Working Paper" on the top left of the first page in letters larger than the text;

(3) Protected per the assigned classification level; and

(4) Destroyed when no longer needed in accordance with procedures outlined in chapter 12 of this instruction.

6. Top Secret Working Papers. The accounting, control and marking requirements prescribed for a finished document will be followed when working papers contain Top Secret information.

EXHIBIT 7A

TOP SECRET AUDIT AND INVENTORY

1. An inventory of all Top Secret material will be conducted at change of directorate TSCO, and at least once annually. Annual report is due to DNS-34 in February of each year.

2. Change of directorate TSCO inventory report is forwarded to DNS-34 with the appointment notice as changes occur. (For change of directorate TSCO, relieving directorate TSCO will conduct the inventory.) Top Secret records are to be audited to determine completeness and accuracy.

3. Publications distributed under the Communications Security Material System will be sighted and accounted for per EKMS. Inventory listing will include: control number assigned, copy number, originator, serial number, date, document title and/or subject.

4. Prior to conducting an inventory of Top Secret material, audit the records as follows:

    a. Use the last inventory of holdings.

    b. Add all incoming and outgoing material since the last inventory, as indicated by higher sequence control log sheets.

    c. Delete the material transferred or destroyed since the last audit as determined by records of destruction, receipts, or completed control log sheets.

    d. List the remaining documents as the audit Top Secret material accountable (for inventory) by the command.

5. The OPNAV security serviced activities' TSCO will provide divisional ATSCOs with list of their holdings (see exhibit 7B). The divisional ATSCOs will inventory the material held and report the results to the command's TSCO. (See exhibit 7C.)

6. Inventory all Top Secret material listed in the current audit by physically sighting each document on the directorate inventories. The directorate TSCO will report the results of the inventory by memo to DNS-34.

7. Detachment/Separation of OPNAV Personnel

SAMPLE

a. Prior to personnel from OPNAV security serviced activities being separated or transferred from the command, the directorate TSCO or ATSCO will verify that the member does not hold any Top Secret material.

b. Designated TSCOs or ATSCOs being separated or transferred from the command will inventory all Top Secret material and document turnover with relief in official correspondence. The relieving TSCO or ATSCO will participate in the inventory.

SAMPLE

EXHIBIT 7B

TOP SECRET AUDIT AND INVENTORY

5511
Date

MEMORANDUM

From: Directorate Top Secret Control Officer
To: (Divisional) Assistant Top Secret Control Officer

Subj: DIRECTORATE TOP SECRET INVENTORY

Ref: (a) OPNAVINST 5510.60N

Encl: (1) Listing of Top Secret Holdings

1. According to my records, you have custody of the Top Secret documents listed in enclosure (1). Please conduct an inventory per reference (a) and report results via endorsed memorandum.

_____
(Signature and date)

SAMPLE

EXHIBIT 7C

5511
Date

MEMORANDUM

From: (Divisional) Assistant Top Secret Control Officer
To: Directorate Top Secret Control Officer

Encl: (1) Listing of Top Secret Holdings

1. I have inventoried and physically sighted the Top Secret documents listed on enclosure (1) in my custody.

2. The following discrepancies exist:

_____
(Signature and date)

SAMPLE

CHAPTER 8
PRINTING, REPRODUCTION, AND PHOTOGRAPHY

1. Controls on Reproduction

a. OPNAV security serviced activities' will ensure that printing and reproducing of classified material are conducted as authorized by references (b) and (c). Printing and reproducing machines will be clearly marked and posted at the appropriate levels of authorization.

b. Top Secret information will not be reproduced without the approval of DNS-34 and consent of the originating activity. All reproduction of Top Secret material will be accomplished by the activity's TSCO who will report the matter to DNS-34 for accountability and inventory purpose.

c. Secret reproduction equipment will be posted for reproducing classified material prominently displaying signs on or near the equipment to advise users. Placards are available in the OPNAV Security Office, or the Security Coordinators can produce placards locally as reflected at exhibit 8A. Reproduction machines should be located within areas that are easily observed to ensure that only authorized copies are being made and the number of copies is kept to a minimum.

d. Apply the same security controls to reproduced copies of classified documents as the originals showing classification and other markings which appear on the original material. Double-check all reproduced material and ensure reproduced copies are clearly and properly marked.

e. If the reproduction equipment is networked to other IT systems or equipment, the whole network must be provided security protection and approved to process classified material at the highest level of classified material reproduced.

f. Before permitting un-cleared maintenance personnel access to or releasing reproduction equipment that has been used for processing classified material, inspect the equipment to clear cache memory and ensure that no classified material has been left in the equipment.

2. Reproduction/Copiers. Copiers, facsimile equipment or similar devices using non-secure or unencrypted telephone lines will not be used to transmit classified information.

a. Digital copiers may contain a hard drive capable of maintaining and storing an image of personal information or sensitive data. Copiers will not be turned in for disposal or maintenance until the hard drive is swept clean.

b. Hard drives must be turned in to OPNAV Security Office for sweeping of hard drives. Alternative is to document hard drives turned in to DNS-44 or for destruction.

3. Requirement for Photography and Imaging Technology in Pentagon and Related NCR Facilities

a. Models of cell phones have been proven to compromise classified data introducing major security risks.

b. Unless proper authorization has been obtained in advance from DoD or Navy components occupying a space, the use of photographic or imaging devices is forbidden in the Pentagon or DoD leased buildings. The following rules apply:

(1) Persons on official DoD photographic/video-graphic missions must use DoD authorized equipment.

(2) Members of such missions on DoD property must follow previously established ground rules.

(3) Cameras/imaging devices may be brought on/in those facilities only after proper vetting, and used only with the permission of the component to which a space belongs. For permission in common areas or secured areas, contact PFPA via DNS-34. Otherwise camera equipment is unauthorized.

(4) Possession and use of a camera or imaging device in any area where collateral classified work is performed requires specific permission from the Security Coordinator of that office.

(5) Unauthorized use of cameras and imaging devices on/in DoD facilities can lead to loss or suspension of security clearances, or more serious administrative and judicial action.

(6) The officers of PFPA are empowered by their evidence collection duties to direct owners of cameras/imaging devices used in an unauthorized manner to remove and hand over the film or storage media in such equipment, or to conduct an on-the-spot review of the images just recorded.

EXHIBIT 8A

SIGN FOR POSTING AT REPRODUCTION MACHINE
(COLOR RED)

THIS MACHINE MAY BE USED FOR PRODUCTION

OF MATERIAL CLASSIFIED UP TO

SECRET

REPRODUCTION MUST BE APPROVED BY:

· ENSURE THAT ORIGINAL AND ALL COPIES ARE REMOVED FROM MACHINE PRIOR TO DEPARTURE

· ENSURE THAT CLASSIFIED MARKINGS ARE LEGIBLE. REMARK ALL DOCUMENTS ON WHICH THE MARKINGS ARE UNCLEAR

· IN THE EVENT THIS MACHINE SHOULD MALFUNCTION, CHECK TO ENSURE THAT ALL COPIES HAVE BEEN REMOVED

SAMPLE

CHAPTER 9
DISSEMINATION OF CLASSIFIED MATERIAL

1. Basic Policy

a. OPNAV security serviced activities will establish procedures for disseminating classified material originated or received by their offices, to limit outside dissemination to those activities having a "need to know" and to reflect any restrictions imposed by originators and higher authority. Procedures will be issued as a part of the command's internal security instruction in chapter 1 of this instruction and will include:

(1) As a minimum, an annual review of classified material distribution lists to ensure classified material is disseminated on a strict "need to know" basis; and

(2) Removal of recipients without continuous access or need for classified material.

b. OPNAV security serviced activities will ensure that material prepared for public release does not contain classified information or sensitive technical data. Policies and procedures governing public release of official information and the circumstances under which a security review is required are detailed in reference (n).

2. NATO Material

. See reference (h) for guidance on dissemination of NATO information.

3. Classified Material

(a) Top Secret material originated within the DoD will be disseminated in accordance with Volume 3 to reference (b). Members requesting dissemination out of DoD will provide the written consent to the cognizant TSCO with the request.

(b) Secret or Confidential material originated within the Navy may be disseminated to other departments and agencies of the Executive Branch of the government unless specifically prohibited by the originator.

4. Dissemination to DoD Contractors. Procedures for dissemination of classified information and material to DoD Contractors are contained in chapter 14 of this instruction.

5. Disclosure to Foreign Governments and International Organizations.

a. Authority for dissemination of classified information to foreign governments and international organizations is centralized at Navy International Program Office as outlined in reference (o).

b. Personnel will avoid any actions that creates the false impressions that the Navy or U.S. Government is willing to enter into any arrangement with a foreign government leading to the eventual disclosure of Classified Military Information (CMI) or Controlled Unclassified Information (CUI).

6. Dissemination to Congress. Information regarding disclosure to Congress is contained in reference (b), volume 3.

7. Classified Material Disseminated to Commands Outside of OPNAV. Classified material disseminated to commands outside of OPNAV will include an OPNAV 5511/10 Record of Receipt (tracer card) for purpose of follow-up to ensure intended recipient received and return the receipt to the OPNAV originator.

CHAPTER 10
TRANSPORTATION OR TRANSMISSION OF CLASSIFIED MATERIAL

1. Basic Policy

a. Classified information will be transported and/or transmitted either in the custody of an appropriately cleared individual, by an approved communications system, or courier per reference (b) volume 3.

b. The term transportation refers to movement of classified information or via car, bus, train, ship, or plane.

c. The term transmission refers to communications of classified information by electronic means via approved telephone, email, fax, video, or teleconference.

d. The hand-carrying of classified material outside of the local metro-Washington D.C. area requires DNS-34 authorization per chapter 6.

2. Top Secret. Top Secret information will be transported or transmitted only by:

a. The Defense Courier Service (DCS) - refer to section 8 of this chapter for instructions.

b. Authorized U.S. government courier services

c. Cleared and designated U.S. military personnel or Government civilian employees traveling on a United States owned passenger aircraft or ship, controlled or chartered by the Government or a DoD contractor.

d. Electronically over an approved secure communications system (i.e., an authorized cryptographic system).

3. Secret. Secret information will be transmitted by:

a. Any of the means approved for the transmission of Top Secret, except that Secret material may be introduced into the DCS only when U.S. control of the material cannot otherwise be maintained.

b. USPS registered mail within and between the United States and its territories.

c. USPS registered mail through Army, Navy, or Air Force postal service facilities, outside the area described in subparagraph 3b above, as:

(1) Provided the mail does not pass through a foreign postal system or any foreign inspection, or via foreign airlines.

(2) The material must remain under U.S. control.

(3) If the material is introduced into a foreign postal system, it has been subjected to compromise.

d. USPS express mail for transmission between U.S. Government activities and between U.S. Government activities and contractors, within and between the United States and its territories.

(1) The use of USPS express mail is permitted when it is the most cost effective, risk managed method of transmittal, given the constraints of time, security and accountability.

(a) Because of the cost, use of the USPS express mail must be approved in advance by DON Headquarters mail centers.

(b) The use of Federal Express for transmittal of classified information can be used as an alternative.

(2) The USPS express mail and Federal Express envelope may serve as the outer wrapper and prepared per section 7.e. below.

e. Designated express delivery holders of the GSA contracts for overnight domestic express delivery of Secret and Confidential material. See DUSN (P)/SD web site at http://www.secnav.navy.mil/dusnp/Pages/Default.aspx for updated listing. These services are prohibited for weekend delivery.

f. Electronic means over approved communication circuits.

4. Confidential. Confidential information will be transmitted by:

a. Any means approved for the transmission of Secret material; however, use of the USPS for Confidential material is governed by the following:

(1) USPS registered mail will be used:

(a) For NATO Confidential;

(b) To and from FPO/APO addresses located outside the United States and its territories; and

(2) USPS first class mail will be used between DoD activities anywhere in the United States and its territories.

(3) Certified or registered mail must be used when sending Confidential mail to the State Department for forwarding by diplomatic pouch. If certified mail is not available, registered mail will be used.

b. In the custody of commanders or masters of ships of U.S. registry who are U.S. citizens as outlined reference (b), volume 3.

5. Telephone Transmission. Classified telephone conversations must be permitted only over secure communication circuits approved for the classification level of the information being discussed. Every attempt must be made to ensure that the classified information is not compromised to unauthorized personnel. All unclassified telephones will be labeled with "do not discuss classified information," DD Form 2056 Telephone Monitoring Notification Decal markings.

6. Receipt Systems

a. Transmit Top Secret material under a continuous chain of receipts.

b. Forward Secret material with a Record of Receipt, OPNAV 5511/10, between directorates, commands and other authorized addresses. Failure to sign and return the OPNAV 5511/10 receipt to the sender may result in a report of possible compromise or a command OPNAV 5511/5 Security Violation Report.

c. OPNAV 5511/10 receipts for Confidential material are not required except when the material is transmitted to a foreign government (including embassies in the United States). A receipt is required for all classified packages hand carried to the U.S. Senate.

d. The sender of the material will attach OPNAV 5511/10 to the inner cover.

(1) Receipt forms will be unclassified and contain only the information necessary to identify the material being transmitted.

(2) Top Secret receipts will be retained for 5 years and Secret receipts will be retained for 2 years.

(3) When wrapping support is required by DNS-34, bring the receipt form to the security office during processing and wrapping of the outgoing classified material.

7. Transmission

a. Transmit of classified material in accordance with to the requirements of reference (b), volume 3.

b. Transmit FOUO/(CUI) and SBU in accordance with reference (b), volume 4.

c. Addressing of Classified Material

(1) Classified material must be addressed to an official Government activity or DoD contractor and not to an individual. An attention line may be used to include office code or department to aid in internal routing. The individual's name may appear on an attention line on the inner envelope. Consult with DNS-34C for more details and support preparation for mailing classified material.

(2) Consult the following for complete and correct mailing addresses and mailing instructions:

(a) Current issue of the SNDL via Department of the Navy Issuance Web site https://doni.documentservices.dla.mil contains the official list of Navy fleet and mobile units, shore activities and their administrative addresses.

(b) The Defense Security Service (DSS), Industrial Security Facility Data, Facility Verification Request (DSS, ISFD, FVR) is the central activity for verification of DoD contractor facilities facility clearance, safeguarding capability and correct classified mailing address. The DSS ISFD FVR can be reached as follows:

Defense Security Service
ISFD FVR
2780 Airport Drive, Suite 400

ATTN: Customer Service
Columbus, OH 43219-2268

d. The inner envelope or container will show the address of the receiving activity.

e. An outer envelope or container will show the complete and correct address of the recipient and the return address of the sender.

8. Defense Courier Service (DCS)

a. Operational control of global courier activities is exercised by DCS, Fort George G. Meade, MD, with a Pentagon substation operating out of the Remote Delivery Facility.

b. Incoming: All deliveries will be picked up by the OPNAV, Top Secret control sections: DNS-34C, (703) 697-l156). Any DNS-34 personnel who are listed on a qualified DCS Form 10 may pick up or deliver DCS material to the Pentagon substation.

c. Outgoing: DNS-34C is responsible for entering material into the DCS system per reference (p).

CHAPTER 11
SAFEGUARDING AND SECURITY STORAGE

1. Responsibility for Safeguarding

a. Members of OPNAV security serviced activities will safeguard classified material at all times as delineated reference (b), volume 3. Classified material will be locked in approved storage containers whenever it is not in use or under the direct observation of authorized persons.

b. Personnel with an appropriate eligibility determination and "need to know" are granted access to classified information or spaces.

c. Personnel will also be aware of and follow procedures which ensure that unauthorized persons do not gain access to classified information.

d. Personnel will only remove classified material from designated offices or working areas in performance of their official duties.

e. Personnel will be authorized to remove classified material from designated areas for work during off duty hours with advance approval from DUSN(P)/SD when it is mission critical. Specific security measures such as IT equipment and associated storage media are required.

(1) Approval will be staffed by DNS-34 for final approval in accordance with Reference (c) after appropriate security measures are met to provide adequate protection, and safeguard is established for classified storage. A list of the material removed will be kept at the command.

(2) Ultimate approval authority for overnight residential storage of classified material resides with DUSN (P)/SD.

f. Residential secure terminal equipment will be installed in a private residence when operational requirements are directed and cleared by the authorized EKMS manager. All residential classified network connections must be certified and accredited in accordance with reference (v) and reference (q). The following security requirements must be followed:

(1) The terminal must be used only by the person for

whom it was installed.

(2) The KOV 14 card must be removed from the terminal following each use and kept in the personal possession of the user or stored in an approved security container.

(a) As indicated above, GSA-approved security container must be furnished for residential storage of classified information.

(b) Written procedures will be posted for appropriate protection of the information.

(3) The terminal will be returned when requested by the EKMS manager, for inventory, scheduled maintenance and at termination of home services.

(4) Immediately report the loss of a terminal or KOV 14 card to the EKMS manager.

(5) When communicating in the secure mode, ensure surroundings will not result in the compromise of classified or eavesdropping.

2. Security Containers

a. General

(1) The custodians' name must be indicated on an SF 700 Security Container Information and posted on the inside of the container door or combination lock drawer. The custodian bears primary responsibility for compliance with security procedures relating to the container and its contents.

(2) Security containers with wheels affixed are not authorized for storage of classified material. One-drawer containers must be fastened secure to prevent unauthorized removal.

(3) SF 701 Activity Security Checklist and SF 702 Security Container Checksheet must be posted in plain and obvious sight. SF 701 must be posted on the inside of the space on the door. SF 702 must be posted external of the space entrance door near the card swipe for the entrance door.

b. Control

(1) When new storage equipment is received, it will be coordinated through the SECNAV Lock Shop under DNS-34's guidance for inspection, numbering and combination setting.

(2) To ensure a complete and accurate inventory is maintained, no container will be moved from its assigned space without prior written approval of DNS-34.

(3) Requests for additional security containers will be submitted as follows:

(a) Via memorandum or e-mail to DON/AA, Facilities' Material Handling Unit.

1. A written verification on each request will show a current physical security survey has been completed by DNS-34 and the Locksmith.

2. The memorandum must include room number and type of container desired, as well as any further justification.

(b) Route the memo to DON/AA, Facilities' Material Handling Unit, copy to DNS-34.

(c) When the security container is delivered, the custodian must request a new combination change by contacting the Lock Shop.

(d) After the combination is changed, the custodian will complete a new SF 700.

(4) Excess security containers must be reported promptly to DNS-34. They must be returned as follows:

(a) Submit a memorandum to DNS-34. Ensure security container and room numbers are on the request.

(b) Remove all classified material.

(c) Locksmith will change or request a contractor to change the combination to factory setting.

(d) Locksmith will respond to inspect the security container and upon completion of the inspection, will notify DON/AA, Facilities' Material Handling Unit.

(e) The material handling unit will pick up the

security container and return it to inventory.

(5) DNS-34 will be notified immediately should any doubt arise concerning the state of repair or suitability of any security storage equipment or open storage area. When problems arise and are not immediately reported, the possibility of lockouts or improperly secured containers may exist.

3. Combinations

a. Protecting and Storing Combinations. The combination will be classified at the same level as the highest classification of the material authorized for storage in the container.

(1) Use SF 700 Part 2, as specified in section 10 of this chapter, to record the combination and other required data.

(2) If another record of the combination is made, the record must be marked as required by reference (b), volume 2.

(3) Security containers, vaults, secure rooms and other authorized storage containers must be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

(4) A record of the names of persons having knowledge of the combination must be maintained.

b. Changing Combinations. Consult the locksmith for combination change to security containers. Combinations must be changed:

(1) When containers/locks are first placed in use:

(2) An individual knowing the combination no longer requires access, unless other sufficient controls exist to prevent that individual’s access to the lock.

(3) The combination has been subject to possible compromise or the security container has been discovered unlocked.

(4) The container or the padlock is taken out of service. Built-in combination locks will be reset to the standard factory combination. Combination padlocks will be reset to standard factory combination.

c. When selecting combination numbers, sequential numbers (i.e., multiples of 5, simple ascending or descending arithmetical series) and personnel data, such as birth dates and SSNs, will not be used.

(1) The same combination will not be used for more than one container in any one open storage area or secondary control point.

(2) When setting a combination, numbers will be used that are widely separated by dividing the dial into three parts and using a number from each third as one of the combination numbers.

d. After the combination is changed, the requesting office will submit a new SF 700. Copy 1 of the SF 700 will be affixed to the inside of the container on the combination lock drawer. Custodian will try the new combination before closing the container.

4. Locking Procedures. When securing, storage containers will be locked without haste, and re-checked. Use the following procedures:

a. Safes. Firmly shut door or drawer and rotate the combination dial at least four complete revolutions in one direction. Check and re-check.

b. Responsibility for securing is assigned to the custodian of each container. In the designated custodian's absence, an alternate custodian must be designated and specifically charged with the responsibility for proper securing of the container.

5. OPNAV Locksmith Services.

a. The SECNAV Lock Shop (DNS-34) is responsible for all lock work, combination locks on doors and security containers assigned. This responsibility includes those offices located outside the Pentagon in swing spaces, and other Metro Washington OPNAV and SECNAV assigned spaces.

b. The SECNAV Lock Shop (DNS-34) will provide keys for personnel within the Pentagon with the approval of the Security Coordinator.

c. Lost, stolen, damaged or misplaced keys should be

promptly reported to the Lock Shop (DNS-34).

6. Areas Protected by Electronic Alarm Systems. Areas protected by electronic alarm systems and procedures for opening and securing alarm areas will be per reference (b), volume 3, enclosure (3).

7. Unalarmed Work Spaces. After normal working hours, unalarmed spaces will be locked with a deadbolt lock. Electrically activated cipher locks do not afford the degree of protection required for classified equipment. These locks may be used during normal duty hours for access control purposes only.

8. Care of Working Spaces

a. During working hours, to prevent access to classified information by unauthorized persons, monitor the entrance to office spaces and do not give un-cleared personnel freedom of movement within the office space. Escort visitors (including cleaning personnel) and question unescorted strangers found within the space.

(1) When classified documents are removed from storage, they will be kept under constant surveillance, face down and covered in accordance with procedures outlined at chapter 4.

(2) All items containing classified information will be destroyed (placed in burn bag) after they have served their purpose.

b. Top of security containers should be cleared of extraneous material, distinctive cover sheets should be used, and classified material should never be placed in desks.

9. Security Checklists

a. An SF 701 Activity Security Checklist must be used to validate security checks at the close of each duty and/or business day to ensure that any area where classified information is used or stored is secured.

b. Forms may be acquired per appendix (C) of this instruction and held for reference for 1 year after the last entry.

10. Key and Lock Control

a. General. Primary responsibility for key control rests

with the Space Custodians, who will act as the Key Control Officer for individual spaces. Each Security Coordinator will act as oversight for his/her organization and will be responsible to the Key Control Officer for key control policy matters.

b. The Lock Shop and DNS-34 maintain a master key for all Navy spaces, which is available upon request for opening of spaces.

c. Duplication of Keys. Security keys will not be duplicated except through the Key Control Officer or Security Coordinator. Unauthorized duplication could result in administrative actions.

CHAPTER 12
DESTRUCTION OF CLASSIFIED MATERIALS

1. General.

a. The Director, Washington Headquarters Service, Physical Security Division, publishes policy for the destruction of classified material within the Pentagon, Crystal City, Navy Support Facility, and OPNAV swing space clientele at the Washington Navy Yard.

b. The Director directs the destruction of classified material through the Pentagon Incinerator Facility while developing procedures and scheduling the use of the facility. Specific schedules and questions may be directed to the incinerator facility at (703) 695-1828.

c. Before destroying any record, classified or unclassified, the person carrying out the destruction process must review appropriate Navy record management program document to determine the life cycle of the record about to be destroyed. Document destruction through use of OPNAV 5511/12 Classified Material Destruction Record.

(1) No record must be destroyed before its approved time.

(2) If emergency destruction is required when a state of crisis exists or is threatened, follow the guidance found at paragraph 6.

2. Procedures

a. Classified material must be placed in burn bags at the Navy office level. Commands are encouraged to have two persons responsible for transporting burn bags to the Pentagon remote Delivery Facility (RDF) or pre-arranging for special pick up points as arranged by the incinerator facility. Burn bags are to be turned in at the Pentagon RDF between 0900 to 1000, or 1100 to 1200 daily.

b. All bags delivered to the RDF should be documented on a DD 2843 Classified Material Destruction Record.

(1) Bags are limited to being three-quarters full and no more than 10 pounds.

(2) Bags must be marked using a black marker to show office, point of contact, phone number and highest classification level of information in the burn bag, as well as the serial number (i.e., 1 of 3, 2 of 3, etc.).

(3) Any bag containing personal data will be marked with "For Official Use Only (FOUO) – Privacy Sensitive – Any misuse or unauthorized disclosure may result in both civil and criminal penalties."

c. Classified IT storage media (e.g., hard drives) cannot be declassified by overwriting. Sanitization (which may destroy the usefulness of the media) or physical destruction is required for disposal.

(1) Hard drives must be placed in a separate burn bag and identified as such. Bulk turn-in, outlined para 2., b. above, is on last Thursday of the month only.

(a) Limit hard drives to five hard drives per bag.

(b) Media, such as Compact Discs (CDs), cassettes or Video Cassette Recorder (VCR) tapes may be mixed in the burn bag with papers.

d. Cross cut shredders, identified on the NSA Evaluated Products List of approved shredders, will be purchased and used as an alternative to burn bags.

3. Destruction Reports. All personnel will record the destruction of Secret and above material for documentation.

a. The cognizance directorate TSCO or alternate must accomplish destruction of Top Secret material. Two witnesses will execute the record when the information is destroyed. Top Secret destruction records must be retained for 5 years.

b. Records of destruction are not required for Secret and Confidential information except for special types of classified information per reference (b), volume 3. A record of destruction is good practice and should be maintained for a minimum of 2 years when done.

4. Message Traffic

a. Unclassified message traffic, except NNPI, does not have to be destroyed as classified material. Classified and

unclassified message traffic will be destroyed through use of burn bag to ensure efficient handling and to preclude inadvertent disposal of classified and sensitive information. FOUO messages will be destroyed by placing them in a burn bag to provide protection for any sensitive subjects or personal data and to preclude public disclosure.

b. Classified messages are distributed via SIPRNET by the JCC to customers per an established restricted profile to individuals vice public folders. Secret messages must still be destroyed by authorized means through burn bag use or shredding by authorized persons.

5. Destruction of CMS Material. COMSEC and other CMS material will be destroyed by designated command EKMS personnel, under NCMS, Washington DC, using the SF 153 COMSEC Material Report in accordance with EKMS-1, CMS Policy And Procedures. Completed SF 153 must be turned in to the CNO EKMS Manager, Naval Communications Material Security, Washington, DC.

6. Emergency Action Procedures

a. Mass destruction or total removal of classified material is not considered feasible within OPNAV security serviced activities. The following instructions govern emergency action procedures for the protection, removal, and destruction of classified material during a fire, natural disaster, civil disturbance, or enemy action.

b. Emergency procedures will be implemented at the direction of the Director, PFPA, or GSA building manager via Computer Based Emergency Notification System (CENS) or "Big Voice" intercom announcements. In the event of the absence of the above, the senior individual present will direct emergency procedures. For those personnel not physically located in the Pentagon, emergency procedures are established by the occupant emergency official and building manager.

c. Procedures. Upon receipt of implementing instruction:

(1) Classified material will be returned to authorized security containers which will then be locked and left in place.

(2) Personnel will remain at their duty position pending receipt of further instructions.

(3) In the event of natural disaster (i.e., storms, earthquake, or fire, etc.), necessitating evacuation of personnel, classified material will be secured in authorized storage containers.

d. Destruction. OPNAV security serviced activities physically located within the Pentagon are exempt from the emergency destruction of classified material. Offices not located in the Pentagon need to establish priorities of emergency/destruction which are consistent and relative by level of classification (i.e., Priority 1: Top Secret, Cosmic Top Secret Atomal and Cosmic Top Secret; Priority 2: U.S. Secret, NATO Secret Atomal and NATO Secret; Priority 3: U.S. Confidential, NATO Confidential Atomal and NATO Confidential; Priority 4: FOUO, U.S. Unclassified requiring operations security protection, NATO Restricted, and NATO Unclassified). COMSEC, codeword, and special access material are prioritized accordance to security classification levels.

e. Relocation. Relocation will generally be limited to the relocation of personnel and material required for operations in accordance with contingency plans.

f. Safety. In the implementation of above procedures, the personal safety of individuals must not be jeopardized.

g. Police. PFPA is responsible for protection of the Pentagon, its occupants and Government and private property. DNS-34 interfaces with PFPA and, in consonance with guidelines, administers security enforcement procedures within OPNAV security serviced activities through the Security Coordinators.

h. Reports. Post event debriefing is required in the event of any emergency. Reporting will include all details surrounding the emergency, including extent of compromise and possible compromise, as applicable. Reporting will be accomplished without delay, through command channels to DNS-34 on behalf of the Director, Navy Staff. Use format contained in reference (b), volume 3, enclosure (6).

i. Post copy of emergency action procedures correspondence within work areas and alert all personnel during annual security refresher training.

CHAPTER 13
VISITS AND MEETINGS

1. General

a. Basic policy regarding visits and meetings can be found at volume 3, reference (b). Upon arrival, visitors must check-in with the command's Security Coordinators for initial briefing and further guidance.

b. For security purposes, the term visitor applies to:

(1) Any person who is not permanently attached by orders, or an OF 8 Position Description, or employed by the command.

(2) Personnel on temporary additional duty.

(3) Reservists, stashes, detailed Inter-governmental Personnel Act (IPA), concessionaires and contractors are also considered as visitors (appointed senior IPAs are treated as permanent employees).

(4) Un-cleared members and support staff including cleaning personnel, movers and repair technicians are visitors requiring escort, and movement must be controlled and escorted at all times to ensure that access to classified information is not disclosed.

c. JPAS is the DoD's official system of record for classified visit requests. Personnel will not hand carry their own visit request(s) as proof of clearance.

2. Outgoing Visits

a. JPAS will be used for personnel security administrative functions, including the administration of visits involving access to classified information. Visit requests will be submitted through JPAS only within DoD. Security Coordinators or Assistant Security Coordinators will verify accuracy of JPAS data and alert appropriate host activities. Visit requests transmitted via electronic mail must be transmitted from the Command Security Manager to the attention of the Security Manager of the command or DoD contractor facility to be visited.

b. Security Coordinators or Assistant Security Coordinators sponsoring the visitor are responsible for ensuring and

validating the accuracy of the access and affiliated data in JPAS before initiating the visit request. The visited command releasing classified information is responsible for verifying "need to know" and for positively identifying the visitors. Technical point-of-contact at visited command is required. Visit requests submitted through JPAS will not be accepted if they do not reflect accurate access documentation including the "Nondisclosure Agreement and accurate affiliation documentation including appropriate point of contact and Security Management Offices (SMO) information.

3. Incoming Visits

a. DNS-34 is the central point for policy and direction on incoming visit requests from all outside activities. Commands receiving visit requests directly will forward them to DNS-34 only to document the requirement for building badges.

(1) OPNAV security serviced activities receiving visit requests from other DoD activities or Government organizations will process and file them appropriately for documentation of clearances, access and building passes.

(2) Visit request files are subject to periodic commands security inspection by DNS-34.

(3) Incoming visit requests from contractor facilities must meet the same JPAS or other electronic documentation as Government personnel.

b. Before access to classified information may be granted to a visitor, the host office must:

(1) Check visitor ID (i.e., Government/contractor picture ID badge or drivers' license).

(2) Have on file a valid visit request with the visitor's security clearance endorsed by either DNS-34 or command's Security Coordinator.

(3) Refer to chapter 14 of this instruction for in-depth information regarding access and classification specifications by contractor personnel.

4. Visits to DOE Activities

a. DOE Request for Visit or Access Approval, DOE F5631.20 Form, will be completed for visits to DOE activities and related contractors. The initiating office will forward to DNS-34 the completed form, and appropriate phone number, 3 days in advance to allow sufficient time for processing.

b. The "To" address block will be filled in with the address of the appropriate DOE activity or contractor facility, unless the visit requires access to weapons related RD or CNWDI. In such cases, the requesting office will leave the "To" block to be completed by DNS-34.

c. Access certification, briefing and debriefing requirements of chapter 2, exhibits 2C through 2G, of this instruction must be met prior to forwarding visit requests for CNWDI and RD accesses. Reference (k) applies.

5. Visits by Representatives of the Government Accountability Office (GAO). Properly cleared and identified representatives of GAO may be granted access to classified DON information in the performance of their assigned duties and responsibilities per reference (b), volume 3.

6. Visits by Foreign Nationals

a. Policy and procedures for classified or unclassified visits by foreign nationals are described in detail in reference (o). Policy and procedures for visits of nationals from communist controlled countries are contained in reference (r).

b. Visits by foreign nationals, including foreign temporary exchange officers, which will involve substantive technical discussions or the disclosure of classified information require the approval of the Navy International Programs Office (IPO-O1B2). Coordination with Navy Foreign Liaison (OPNAV (N2L)) is required for issuance of building passes. A copy of the personnel exchange agreement and delegated disclosure authority will be provided to DNS-34.

7. Classified Meetings

a. Any meeting which will involve the disclosure of classified information must be held at a Government installation or cleared DoD contractor facility where adequate physical security and procedural controls have been approved.

b. See reference (b), volume 3, for detailed responsibilities that impact upon security sponsorship of classified meetings, conferences, seminars, symposiums and conventions, specific security procedures for classified meetings and procedures for obtaining clearances for non-government attendees.

c. Requirements for classified meetings at base theatres, school auditoriums and in any unsecured classrooms will be coordinated with DNS-34. Further coordination of Technical Surveillance Countermeasures (TSCMs) support is required.

d. Conference Rooms

(1) Protection of classified information within a conference room is the responsibility of the official sponsoring the meeting. Prepare a security plan to minimize risk and to publish and manage classified documents and discussions in accordance with reference (b), Volume 3.

(2) The official requirement to hold a Top Secret meeting in a conference room which is not alarmed will notify DNS-34 at least 30 working days in advance for completion of technical survey.

(3) Meetings classified Secret or above require a monitor while the conference is in session. Access control is provided to ensure that personnel attending the conference have clearances equal to or higher than the level of information to be discussed and a “need to know.”

(4) Telephones located in conference rooms must be disconnected; no cell phones allowed at any time.

CHAPTER 14
INDUSTRIAL SECURITY

1. General. Reference (s) provides the minimum safeguarding requirements for management of OPNAV's Industrial Security Program. The DD 254 Department of Defense Contract Security Specification with its attachments and supplement is the authorized means for providing security classification and guidance to a contractor with a classified contract. Classified information is the property of the U.S. Government. The Government User Agency (UA) is responsible for providing contractors all security classification guidance necessary to properly classify information and material produced under the terms of the contract.

2. Classified Contracts. A classified contract is one which requires access to classified information by the contractor in performance of the contract. A contract may be classified even though the contract document itself or task is not classified. A DD 254 must be prepared following the provisions of reference (s) by the cognizance program office for each new procurement request which will result in a classified contract. The DD 254 must not be classified.

3. Contract Security Classification Specification (DD 254)

a. Each procurement request which requires access to classified information for contractual performance must be accompanied by a DD 254. The responsibility for preparation of the DD 254 rests with the program office having technical cognizance over the procurement. DD 254s are legal contractual documents and will only specify actual requirements that the contractor needs in full performance of the contract. The DD-254 will be signed by the contracting officer's technical representative and DNS-34 who is designated as Contracting Officer's Representative (COR) by billet (occupation code 0080) as delineated by reference (t).

b. Cognizant technical offices will prepare a draft DD 254 following the instructions provided in this chapter, forward the drafted DD 254, the statement of work, and classification guides to DNS-34 for review and finalizing.

c. OPNAV technical offices will review DD 254s biennially, as well as whenever classification guidance changes. The results of reviews will be provided to DNS-34. Biennial review and/or final DD 254 will not be required when the contract

provides access only to classified information or the contract is a service type contract.

d. When final delivery of the end item has been completed and retention of classified material is requested, a final DD 254 will be prepared. DNS-34 will coordinate requests for retention of classified material, verify "need to know" and any other security or classification matter. Replies to the requestor will be prepared by DNS-34 and a copy will be sent to the cognizant OPNAV technical office.

4. Classified Visits to OPNAV Security Serviced Activities by Contractor Personnel

a. Refer to chapter 13 of this instruction for policy regarding classified visit by contractor personnel.

b. If contract performance is to be in whole or part on-site (within OPNAV spaces), obtain approval of DNS-34 to ensure that all security requirements are addressed. Contractor employees are not attached to the command, therefore, do not come under administrative control of the command. Specific Security issues will be referred back to the contractor Facility Security Officer for handling and reporting to Defense Industrial Security Clearance Office (DISCO). Security issues pertaining to on-site contract performance must be included in the DD 254 or appended as a supplement at item 13, on the DD 254.

5. Dissemination of Classified Material to DoD Contractors

a. Refer to chapters 6 and 9 of this instruction for hand carry and dissemination of classified material to contractor personnel.

b. Classified material must be sent with a letter of transmittal and OPNAV 5216/4 Outgoing Mail Record. The letter of transmittal will contain the contract number under which the classified material is being released. In addition, the releasing office will verify the facility clearance, safeguarding capability and classified mailing address as outlined in chapter 10 of this instruction.

c. Access to classified information by a contractor is normally justified when:

(1) A bona fide contractual relationship exists between the contracting organization and the UA; or

(2) Access is required in connection with pre-contract negotiations; and

(3) The organization has a current facility clearance commensurate with the classification of the information to which access is requested; and

(4) The person(s) for whom the access authorization is intended has a personnel security clearance commensurate with the information to which access is requested; and

(5) The person(s) for whom access is requested has a valid "need to know."

6. Consultant Clearances

a. The information contained in this section refers to those consultants hired under the provisions of the Office of Personnel Management (OPM) but are not paid. Consultant clearance will not be processed unless the consultant is approved and processed via the civilian personnel office.

b. In all cases, personnel security clearances/facility security clearances/classified storage capability for self-employed consultants must be processed in accordance with the provisions in reference (s).

c. Consultants' clearances will be processed by DNS-34. Requests must be submitted to DNS-34 from S/HHRO as all other civilians hired.

d. Access to classified information will not be granted to consultants until the Defense Industrial Security Clearance Office (DISCO) has issued a Letter of Consent (DISCO Form 560) to DNS-34. Although a prospective consultant may have a current valid clearance with a DoD contractor, it is not for use as an OPNAV security serviced activity consultant. A concurrent clearance must be obtained by DNS-34 from DISCO.

e. Security Coordinators will ensure consultants check in and out with DNS-34. Check-out procedures include debriefing, return of CACs, and verification that classified material has been returned to the employing office. DNS-34 will execute a DISCO Form 562 Personnel Security Clearance Change Notification

or execute a final DD 254 to administratively terminate the individual’s clearance.

EXHIBIT 14A
GUIDELINES FOR ON-SITE CONTRACT PERFORMANCE

1. On-site contractor performance require approval and coordination via DNS-34 to ensure all security requirements are addressed. Provide DNS-34 with the "Statement of Work" and drafted DD 254. Contractor employees do not come under administrative control or authority of the Navy. Mandated measures must be included in the DD 254 to hold the contractor responsible for security requirements. Unnecessary performance requirements will increase the contract costs, and will not be specified for performance by the contractor. Having contractor employees on access lists and acting as custodians for classified material/spaces is not encouraged and must only be requested when performance cannot be achieved by other means.

2. Once it has been determined that contract performance is required on-site and the contractor(s) will be responsible for security aspects, the requirement will be included in the DD 254 in item 13 to include applicable security regulations, procedures, instructions, etc. The DD 254 is the only way to enforce the security requirements. A contractor employee cannot be responsible for securing a classified container unless it has been put in writing and applicable security guidance regarding such actions has been documented. IA tasks are the most common duties performed by contractor employees on-site. In these cases, the command IA security program must apply to the contractor and be addressed in the DD 254.

3. A Standard Practice Procedure will be included in sufficient detail to place into effect all security controls required in addition to reference (s) which are applicable to the contract on-site operation.

4. Normally, all defensive security briefings will be provided to the contractor either by DNS-34 or by their contractor facility. However, when required for unique training applicable to only the contractor employee(s) performing contract work on-site, briefings will be provided by the Security Coordinator or Contracting Officer's Technical Representative (COTR). When the contractor employee requires a foreign travel briefing, the PFPA source is available. Notify the contractor facility for record purposes.

SAMPLE

CHAPTER 15
COMPROMISE AND OTHER SECURITY VIOLATIONS

1. General

a. It is the duty of each individual assigned to a sensitive billet to comply with reference (b), volumes 3 and IV, to report loss, compromise or possible compromise of classified and CUI information. Reports of loss, compromise, possible compromise will be to DNS-34 via Security Coordinators.

b. DON unauthorized disclosure (UD) of classified information and CUI guidance is further defined by ALNAV 001/16. Also identified are specific categories of UD which will be documented during preliminary inquiry phase in additional to requirements of reference (b). The investigation official will also specify if the UD was willful, negligent of classified information (NDCI), or inadvertent. Additionally the PI will be marked FOUO indicating portions which warrants protection. A loss occurs when classified information cannot be physically located or accounted.

c. JAG manual investigation (OPNAV report control symbol 5510-6C applies per reference (c), appendix C) is a potential recommendation resulting from a PI to provide a more detailed investigation and recommend disciplinary action or additional corrective action. NCIS is available for investigative assistance.

d. Per reference (b) volume 3, classified information is considered compromised if it has been handled through a foreign postal service, its shipment container has been damaged to expose the content, or it has been transmitted over unprotected communications circuits.

e. Electronic spillage (ES) occurs when classified data are introduced either onto an unclassified information system or to an information system with a lower level of classification, or to a system not accredited with proper safeguard measures. All hands will pay strict adherence to ISSM and NMCI guidance for reporting, scrubbing and recovery of ES in accordance with requirements outlined in chapter 16 of this instruction.

2. Security Violations

a. When DNS-34 has determined that there has been a security violation, OPNAV 5511/5 Security Violation Report will

be sent from DNS-34 to the OPNAV security serviced activities concerned on behalf of CNO (DNS). Command authorities must appoint, in writing, a command official, other than subordinates of potential culprits or anyone involved in the incident, to conduct a PI. A PI will be conducted by the appropriate Security Coordinator or other designated official. To avoid a conflict of interest, no individual involved or suspected of involvement with a security violation will be permitted to act as an inquiry official, nor will inquiry results be reported via any individual involved or suspected with a security violation.

b. PIs will be initiated and completed as soon as possible, not exceed 10 days from receipt of the request, signed by DNS-34, and must:

(1) Coordinated with assigned Legal officials and strictly adhere to the requirements of reference (b), volume 3 and will accurately identify the information lost, compromised or subjected to possible compromise, to include:

(a) Classification of the material;

(b) Identification/serial numbers;

(c) Date;

(d) Originator's contact information and guidance;

(e) OCAs;

(f) Subject;

(g) Downgrading/declassification;

(h) Number of pages/or units of information;

(i) Command's point of contact information; and

(j) Unit Identification Code (UIC) of custodial command.

(2) Determine the circumstances surrounding the incident and identify any requirements for additional command action.

(3) Identify all witnesses to the violation and informally interview them to determine the extent of the violation.

(4) Identify the individual responsible, if possible.

(5) Make an attempt to discover the weakness in security procedures that allowed the compromise or subjection to compromise to occur.

(6) Evaluate the information compromised or subjected to compromise to determine the extent of potential damage to national security, and the action necessary to minimize the effects of the damage.

(7) Include a statement that the NCIS field office, Naval Investigative Service Resident Agency (NISRA), Washington Navy Yard, has been advised and accepted or declined investigation responsibility. Can also contact the OPNAV assigned onboard NCIS support officer to determine if an immediate response is needed.

(8) Establish either:

(a) That an unauthorized disclosure of classified material did not occur (see subparagraph 2c below), or the compromise may have occurred but under circumstances presenting a minimal risk to national security (see subparagraph 2d below); or

(b) That compromise is confirmed and that the probability of damage to the national security cannot be discounted (see subparagraph 2e below).

c. If it is determined that a compromise or possible compromise in fact did not occur, the inquiry will be terminated and report of inquiry will be sent via the OPNAV security serviced activity and DNS-34 to Executive Assistant, Director, Navy Staff (EA DNS). No further reporting is required.

d. If a determination of possible compromise:

(1) Minimal risk is made;

(2) No significant command security weakness is found; and

(3) When formal disciplinary action is not appropriate, the inquiry will be sent back to DNS-34. If DNS-34 agrees that conditions have been met, notification of the originator of the material involved is required. The OPNAV security serviced

activity will notify the DoD originators that no further action will be taken with copy to DUSN (P)/SD. DUSN (P)/SD is the designated authority for notifications of compromises to originators of the material that are outside of DoD.

(4) If DNS-34 does not agree that conditions have been met, concurrence will be sought from EA DNS and a JAG manual investigation will be directed. A copy of the investigation results will be sent via CNO (DNS).

d. Security regulations require that performance rating system of all DON personnel, whose duties significantly involve creation, handling, or management of classified information, include a critical security element on which to be evaluated.

3. Review of Violation Reports. EA DNS will be briefed on all completed investigation reports to ensure that the findings of the preliminary investigation are complete and appropriate corrective action has been taken to preclude reoccurrences. Where insufficient or inappropriate action appears to have been taken, EA DNS will recommend further investigation.

CHAPTER 16
INFORMATION SYSTEM (IS) SECURITY

1. Purpose. To emphasize general computer and other IS security oversight as delineated by the Department of the Navy, and OPNAV IA Program regulations and established PSAG unique requirements for monitoring of IS vulnerabilities.

2. E-Ring Activities. OPNAV activities located on the Pentagon outermost E-ring must be aware of the electronic, line of sight, and other perceived threats that may be directed from adjacent locations to the Pentagon Reservation property or from high points in the near vicinity through the outer windows. Occupants of outlying Navy workspaces will also consider the same threat measures before positioning of computer monitors. In an effort to limit the threat risk, office personnel will ensure placement of countermeasures that would limit threat penetrations from outside of the building. To further reduce the threat, DNS-34, DNS-43, and directorate security coordinators will ensure that workstations are aligned as far from windows as feasible and monitors are oriented perpendicular to the windows and outer walls.

3. Command Responsibility and Authority. DNS-4 is designated to establish computer security policy and ensure program effectiveness and compliance with higher directives. Enforcement of IS security matters, administration of IS and security awareness for Navy personnel assigned to OPNAV resides with DNS-4. Physical security of Navy Information Systems (IS) is provided in accordance with chapter 11 of this instruction and reference (q). Spaces will be certified by DNS-33 as determined in reference (c) for IS employability and use as part of open storage certification process. Security coordinators will work in conjunction with their directorate Assistant Customer Technical Representative (ACTR) to ensure the directorate maintains IS security compliance. ACTRs will be nominated by directorate and designated by DNS-4 in writing per exhibit 16A of this chapter.

4. User Role and Responsibilities. To facilitate compliance with OPNAV IS security policy, user’s roles and responsibilities are provided in reference (d). Users must be aware of the potential threat at all times while utilizing IS hardware and software. In addition to specific guidance provided by above referenced documents, users must:

a. Complete OPNAV 5239/14 System Authorization Access

Request Navy (SAAR-N) and the annual Cyber Security training to facilitate initial access and continued access to Navy ISs.

b. Protect passwords/PINs for systems requiring logon authentication and safeguard passwords/PINs at the sensitivity level of the system for classified systems and at the confidentiality level for unclassified systems. Passwords/PINs will be classified at the highest level of information processed on that system.

c. Virus check all information, programs, and other files prior to uploading onto any Navy IS resource.

d. Immediately report all security incidents, including Personally Identifiable Information (PII) breaches in accordance with local procedures and security regulations.

e. Access only that data, control information, software, hardware, and firmware for which users are authorized access and have a "need to know," and assume only those roles and privileges for which they are authorized.

f. Be subject to monitoring, and further understand that there is no individual right to privacy over the data and communications generated through IS use.

g. Digitally sign and encrypt official e-mail in accordance with current policy.

h. Users must not:

(1) Auto-forward official e-mail to a commercial e-mail account;

(2) Bypass, strain, or test IA mechanisms (e.g., firewalls, content filters, anti-virus programs, etc.) without coordination and written approval from DNS-43;

(3) Introduce or use unauthorized software, firmware, or hardware on any Navy IT resource;

(4) Relocate or change equipment or the network connectivity of equipment without authorization from DNS-4;

(5) Utilize personally owned hardware, software, shareware, or public domain software without authorization from DNS-4;

(6) Upload executable files (e.g., .exe, .com, .vbs, or .bat) onto Navy IT resources without the approval of DNS-4;

(7) Participate in or contribute to any activity resulting in a disruption or denial of service;

(8) Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code;

(9) Utilize Navy IT resources in a manner that would reflect adversely on the Navy (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violation of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service); and

(10) Place data onto Navy IS resources possessing insufficient security controls to protect the data at the required classification.

i. Transfer of data between classified and unclassified systems. Only personnel properly trained and designated, in writing, by the Information Systems Security Manager (ISSM) are authorized to perform data transfers within OPNAV. Each N-Code has Data Transfer Agents (DTAs) designated that are authorized to perform these type of data transfers. Users requesting data transfers between systems must contact their N-Code DTA to obtain the current data transfer policies.

j. Lock workstation and remove CAC/SIPRNet token if stepping away for any period of time."

k. When utilizing a password to access a Navy IS, the user must utilize a combination of two uppercase, two lowercase, two numbers and two symbols in your password (16 characters minimum).

l. Be aware of and report indications of virus infections to NMCI, DNS-34, and DNS-4.

5. OPNAV Outlook Web Access (OWA) Requirements. When an OPNAV user requires remote access to Navy IS, that user should be assigned a government laptop which provides WIFI and/or broadband remote access service or a MOBIKEY device. If the user has not been assigned one of these devices or if the laptop

connection does not provide sufficient remote access, permission may be granted to access NMCI e-mail utilizing OWA and a non-government computer. The following applies to OPNAV OWA access:

a. OPNAV directorates are responsible for validating each user's OWA requirements. The validation process includes coordination with the directorate respective budget coordinator to purchase the required and appropriate CAC reader.

b. Prospective OWA users will be provided the OPNAV User Responsibilities and Acknowledge and the OPNAV Remote Access Request Memorandums by the command ACTR, who will also direct users to the specific Web site for completing OWA training course "NMCI Outlook Web Access (OWA) Policy Training."

c. Permission to use OWA for remote access to unclassified NMCI email can be granted only after the user's directorate has validated the user's requirement and after completion of all required forms and online training.

d. Upon receipt of the completed memorandums and certificate of completion for the online training course, DNS-4 will issue the appropriate middleware for use with the CAC reader. DNS-4 retains all approved requests for OWA access.

e. The directorate authorizing OWA access is responsible for obtaining CAC readers and establishing a process for issuance of CAC readers to their authorized users. CAC readers and associated software will be retrieved from individuals prior to their transfer or when CAC reader use is no longer required. Directorates will confirm and notify DNS-4 when the middleware has been removed from the OWA user's non-DoD computer so the middleware can be returned to inventory or reassigned.

f. All authorized OWA users must comply with all required procedures and computer configuration requirements.

6. Portable Computer Devices Requirements

a. With the proliferation of small portable computer devices, OPNAV personnel must pay close attention to regulations and strictly comply with established procedures for:

(1) Utilization and protection of portable computing devices and removable media;

(2) Cellular phones use and restrictions;

(3) IT wireless security policy;

(4) Policy on photography and imaging technology in Pentagon and related NCR facilities; and

(5) Security of Pentagon computer workstations.

b. Further information is provided as follows:

(1) Reference (t) establishes Navy policy on the use of portable storage devices, such as recordable CD rewritable DVD, flash/thumb drives, memory sticks and mini external hard drives, that can be easily attached and removed from NMCI systems without notice.

(a) Use of Universal Serial Bus (USB) portable electronic storage devices on classified and unclassified IS is as follows:

1. Government owned USB external hard drives are the only USB portable electronic storage devices authorized for utilization on Navy IS. Devices are required to be virus scanned and receive written approval from DNS-4 prior to utilization on any Navy IS; and

2. These devices become permanently classified at the same level of the system unless the device is physically locked to "read only" and when following procedures posted at https://infosec.navy.mil.

(b) Non-USB portable electronic storage devices include: DVDs and CDs-Ready Only Memory. These devices are the only non-USB portable electronic storage devices authorized for use on any Navy Information System. Proper utilization of these devices include:

1. Limited to only those devices required to perform an official DoD, DON or OPNAV operational mission requirement.

2. Must be a Government owned asset (Personally owned devices are not authorized on any Navy IS).

3. Government procured devices are authorized on Navy IS only after the device has been properly scanned and the authorization request has been received and approved by DNS-

4. All portable electronic storage devices will be labeled with overall classification and associated markings using appropriate label.

5. Storage and protection of Controlled Unclassified Information (CUI) consisting of PII individuals requires Data at Rest (DAR) encryption in accordance with DoD guidance.

6. Proper chain of custody procedures are required depending on the overall classification of the device.

7. In the event that classified information or CUI contained on a portable electronic storage device is lost, stolen, or misplaced, DNS-34 and DNS-4 must be notified immediately.

8. Electronic portable storage devices impacted by an ES must be surrendered to DNS-4 and/or NMCI as directed for ES cleanup and mitigation.

(c) Thumb drives, flash drives, flash cards, cameras, cell phones, smart phones, music players, and all other portable electronic storage or recording devices not authorized above are not authorized for use on any Navy IS.

(2) Destruction of all portable storage devices, hard drives, and classified software will be in accordance with procedures outlined in chapter 12 of this instruction and the ACTR designation letter (exhibit 16A). Hard drive destruction will be coordinated with the security coordinator and documented on OPNAV 5239/15 Classified Hard Drive Destruction Log.

(3) Cell phone and other wireless device vulnerabilities:

(a) All cellular devices will be surrendered before entering any space where classified information may be discussed, stored, or processed per paragraph 4.2 of reference (u). Personnel should be aware that some facilities do not have the capability to securely hold cellular devices. All personnel must be aware of inherent cellular device vulnerabilities as follows:

1. Conversations could possibly be monitored

while using the phone;

2. The cellular device could possibly act as a microphone to transmit conversations in the vicinity of the cell phone even when the phone is inactive;

3. The cellular device number could be "cloned" or used by others to make calls that are charged to the user's account.

(b) Information protection begins with each OPNAV officer, sailor, civilian and contractor employee, and all must be mindful of both the threat and systems vulnerabilities. See the command security manager, DNS-4 and security coordinators for posting of requirements and availability of the latest PSAG wireless communications reference documents.

EXHIBIT 16A

5510
DNS-4
<date>

From: Chief of Naval Operations Command Information Officer (DNS-4)
To: Individual Appointed (full name, office code, location and telephone number)
Via: Directorate Head

Subj: DESIGNATION AS NAVY AND MARINE CORPS INTRANET (NMCI) ASSISTANT CONTRACT TECHNICAL REPRESENTATIVE (ACTR)

Ref: (a) Executive Order 13526, 29 Dec 2009
(b) SECNAV M-5510.36, Department of the Navy Information Security Program (ISP) Manual
(c) SECNAV M-5510.30, Department of the Navy Personnel Security Program (PSP) Manual
(d) SECNAVINST 5239.3A, Department of the Navy Information Assurance (IA) Policy
(e) OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program
(f) USSAN 1-70, United States National Security Authority for NATO (USSAN) Instruction (Industrial Security) (NOTAL)
(g) DoD Instruction 5210.2, Access to and Dissemination of Restricted Data and Formerly Restricted Data, 3 June 2011
(h) CNO ltr 5510 N09N2/8U223000 of 7 Jan 2008, Subj: Updated Policy for "Declassify On" Markings (NOTAL)
(i) OPNAVINST 5513.1F, Department of the Navy Security Classification Guides
(j) DoD Manual 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 2006
(k) SECNAVINST 5720.42F, Department of Navy Freedom of Information Act Program
(l) OPNAVINST F5511.35L, Safeguarding Nuclear Command and Control Extremely Sensitive Information
(m) SECNAVINST S5460.3F, Management, Administration, Support, and Oversight of Special Access Programs Within the Department of the Navy (NOTAL)
(n) NAVSEAINST 5511.32C, Safeguarding of Naval Nuclear Propulsion Information (NOTAL)
(o) SECNAVINST 5720.44C, Department of the Navy Public Affairs Policy and Regulations

SAMPLE

(p) SECNAVINST 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives
(q) Naval Information Assurance Publication, IA Pub-5239 -22, Oct 2003
(r) SECNAVINST S8126.1, Naval Nuclear Weapons Security Policy (NOTAL)
(s) DoD Instruction 5200.33, Defense Courier Operations, 19 May 07
(t) OPNAVINST C55l0.159, Guidelines Applicable to Communist Nationals Entering the United States as Non-Immigrant Aliens (NOTAL)

1. You are appointed as an Assistant Contract Technical Representative (ACTR) for all NMCI services required in support of your assigned Directorate. Your period of appointment must be a minimum of 1 year from the date of this letter. In the performance of your ACTR duties, you will become familiar with the guidance in references (a) thru (t). You will represent your Directorate, and coordinate with the OPNAV NMCI Contract Technical Representative (CTR) (OPNAV (DNS-42)). You are also required to coordinate your ACTR duties with your directorate's command security coordinator to ensure full compliance with current security regulations in accordance with reference (d).

2. Your duties and responsibilities as an NMCI ACTR include:

a. Maintaining Directorate's accounts in the following NMCI related on-line tools: Service Request Electronic Form (SReForm); Navy Enterprise Tool (NET); and Information Strike Force (ISF) Tools.

b. Conducting in-processing for all new Directorate personnel to include:

(1) Verifying security clearance with your directorate's command security coordinator;

(2) Providing brief on their security responsibilities;

(3) Determining and ordering NMCI service requirements;
(4) Transferring existing or creating new NMCI user accounts; and

(5) Ensuring OPNAV 5239/14 System Authorization Access Request Navy(SAAR-N) forms are completed and routed to the

Command Information System SecurityManager, DNS-43.

c. Acting as your Directorate's focal point for all NMCI requirements to include:

(1) Assisting Directorate users with submitting trouble tickets;

(2) Preparing Move-Add-Change (MAC) requests; and

(3) Maintaining the NET database for accurate accounting and billing for all Directorate user accounts and NMCI delivered services and assets.

d. Maintaining up-to-date familiarity with NMCI Contract Line Item Numbers (CLINs). They are used in the ordering and accounting of NMCI services and change routinely.

e. Conducting monthly survey of all NMCI services being provided to the Directorate to identify:

(1) New service requirements. Coordinate ordering, funding and delivery with the Directorate and the OPNAV CTR. Verify actual date of full delivery of all NMCI services to provide full invoice accounting to the OPNAV CTR;

(2) Services due for technical refresh. Coordinate replacement schedule with the Directorate and the OPNAV CTR; and

(3) Services no longer required by the Directorate. Coordinate termination and equipment turn-in with the Directorate personnel and the OPNAV CTR. If the services being terminated involve classified material (including classified computers, hard drives, storage devices, etc.), the ACTR must coordinate turn-in with the directorate's command security coordinator and the OPNAV CTR. All classified material handling and destruction requirements must be in accordance with Chapter 12 of reference (d).

f. Supporting the directorate command security coordinator and the Command Information System Security Manager (ISSM), as required.

g. Assisting directorate personnel with contacting the NMCI helpdesk and escalating trouble tickets that are not being resolved in a timely manner. If additional escalation is required to resolve a trouble ticket, the ACTR must coordinate

with the OPNAV CTR.

h. Coordinating any Directorate personnel moves (internal or external to their current office) with the OPNAV CTR prior to actual move to properly plan, document, and ensuring minimal service interruption to the user. Coordination includes but is not limited to:

(1) Providing move details and timelines to the OPNAV CTR;

(2) Submitting requirements for all Pentagon and NCR infrastructure changes; and

(3) Submitting updates to the NET tool and providing MAC for all NMCI hardware asset physical moves and/or NMCI active directory changes.

i. De-activating or transferring all NMCI user accounts upon their departure from the Directorate and/or the command. Submit updates to the NET tool, and provide MAC requests for all NMCI hardware asset physical moves and active directory changes.

j. Ordering new NMCI services and conducting the periodic technical refresh of existing NMCI services. ACTR duties include:

(1) Ensuring the following information is correct in the NET tool: all NMCI SIPRNET and NIPRNET requirements; personal data for each individual user (profile and account information); and asset information, including asset tag number and location.

(2) Ensuring all software applications required for each user are identified correctly and associated with the correct user and asset in the NET tool.

(3) Prior to delivery, coordinating NMCI delivery of any new services, equipment, or software applications with the appropriate Directorate office personnel and the OPNAV CTR.

(4) For SIPRNET desktop computers, coordinating receipt of all classified internal hard drives with the directorate's command security coordinator. Ensure all "chain of custody" paperwork is completed to transfer classified material to the end user.

SAMPLE

3. Proper handling, transfer, and/or destruction of classified NMCI materials in accordance with current security regulations, protocols and procedures are integral to adequately perform the ACTR function. Classified NMCI materials includes all classified hard drives/desktop and laptop computers/storage devices or media. To prevent security incidents, ACTRs will ensure compliance with all requirements outlined in references (a) thru (k) and the following:

a. Contractor personnel, to include NMCI support personnel, are not authorized to hand carry any classified NMCI material out of designated Security Serviced Activity spaces without prior arrangements and approval of the OPNAV Command Security Manager (DNS-34) via their directorate's command security coordinator in accordance with reference (d).

b. Military/government civilian personnel are not authorized to remove any classified NMCI material from their designated office or working area except in the performance of their official duties in accordance with reference (d).

c. Under no circumstances can any personnel remove any classified NMCI material from designated work areas to use during off duty hours, or for any other purpose involving personal convenience, without specific approval of the OPNAV Command Security Manager (DNS-34) via their directorate's command security coordinator in accordance with reference (d).

d. The ACTR must coordinate all service termination and turn-in of classified NMCI material, in advance, with the directorate's command security coordinator and the OPNAV CTR. Ensure all classified material handling and destruction complies with Chapter 12 of reference (d).

(1) For classified desktops and laptops, remove classified hard drives and all classification stickers. When removing the hard disk drive from the chassis or cabinet, also remove any steel shielding material or mounting brackets which may interfere with magnetic fields. Maintain custody of desktops and laptops that have had their hard drives and classification stickers removed within the Directorate secure spaces until proper custody transfer or destruction utilizing OPNAV 5239/15 Classified Hard Drive Destruction Log is coordinated by the ACTR with the Directorate's Command security coordinator and the OPNAV CTR.

(2) Classified hard drives must be placed in burn bags

SAMPLE

that contain no other material. The bags must be clearly labeled as containing hard drives. No more than five hard drives must be allowed per bag.

(3) Classified media, such as CDs, cassettes, or VCR tapes may be mixed in burn bags containing other classified papers and materials.

(4) All burn bags must be protected and stored within the Directorate secure spaces and out of view from the office entrance doors at all times until it is time to deliver to the Pentagon Remote Delivery Facility (RDF) for destruction.

(5) In coordination with the directorate's command security coordinator, record the destruction of all burn bags containing NMCI related classified material at the Pentagon Remote Delivery Facility (RDF), and provide copies to the OPNAV CTR. Components are not considered destroyed until a signed notice of destruction is received from the approved destruction organization.

4. Training is essential for successful performance of the ACTR duties. ACTRs must complete the following training within 90 days of designation. Failure to complete this training will result in this ACTR designation and all authority it grants being revoked until such time as the training is fully completed.

a. Complete the computer-based training modules on the CTR training website: https://www.homeport.navy.mil/training/ctr/

b. Attend an ACTR training session held by the OPNAV CTR. These sessions are conducted on a quarterly and by request basis.

c. Complete the annual Navy Network Warfare Command (NNWC) directed Information Assurance (IA) refresher training on Navy Knowledge Online (NKO).

5. Violations of the referenced instructions and this designation letter.

a. Military personnel are subject to disciplinary action under the Uniform Code of Military Justice (UCMJ), or criminal penalties under applicable Federal Statutes, as well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of the referenced

SAMPLE

instructions and this designation letter.

b. Civilian employees are subject to criminal penalties under applicable Federal Statutes, a well as administrative sanctions, if they knowingly, willfully or negligently violate the provisions of the referenced instructions and this designation letter.

6. Your signature below acknowledges your responsibility as an ACTR for your Directorate. Your support and professionalism are necessary for success of your Directorate's and OPNAV Staff's mission. While each person in your Directorate is individually responsible for their own NMCI accounts, equipment, and actions while using NMCI, your integral involvement in the NMCI ACTR program ensures the continued availability and security of NMCI services for your Directorate, OPNAV and the Navy. You will be notified of any change in this appointment.

Designee's Signature/Date:_____/_____

OPNAV CIO (DNS-4) Signature/Date: _____/_____

Copy to:
Personnel File
OPNAV Command Security Manager (DNS-34)
OPNAV Command NMCI Contract Technical Representative (DNS-42)

.

SAMPLE

APPENDIX (A)

REFERENCES

(a) Executive Order 13526, 29 Dec 2009
(b) DoDM 5200.01-V 1, V 2, V 3, V 4, Feb 24, 2012
(c) SECNAV 5510.36 of June 2016, Department of the Navy Information Security Program (ISP) Manual
(d) SECNAV M-5510.30, Department of the Navy Personnel Security Program (PSP) Manual
(e) DoDM 5200.02, Procedures for the Personnel Security Program, Apr 3, 2017
(f) SECNAVINST 5239.3B, Department of the Navy Information Assurance (IA) Policy
(g) OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program
(h) USSAN 1-07, United States National Security Authority for NATO (USSAN) Instruction (Industrial Security) (NOTAL), 5 Apr 2007
(i) Chairman JCS instruction 3231.01B, 15 Jan 2009
(j) DoD Instruction 5210.2, Access to and Dissemination of Restricted Data and Formerly Restricted Data, 3 Jun 2011
(k) Administrative Instruction (AI) #30 Force Protection of the Pentagon Reservation, 26 June 2009
(l) SECNAVINST 5720.42F, Department of Navy Freedom of Information Act Program
(m) OPNAVINST 5513.1F, Department of the Navy Security Classification Guides
(n) SECNAVINST 5720.44C, Department of the Navy Public Affairs Policy and Regulations, Oct 14, 2014
(o) SECNAVINST 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives, Oct 8, 2004
(p) DoD Instruction 5200.33, Defense Courier Service Program, 30 Jun 11
(q) Naval Information Assurance Publication, IA Pub-5239-22, Sept 2008
(r) OPNAVINST C55l0.159, Guidelines Applicable to Communist Nationals Entering the United States as Non-Immigrant Aliens
(s) DoD Manual 5220.22-M, National Industrial Security Program Operating Manual, 18 Mar 2011
(t) COMNAVNETWARCOM Computer Tasking Order (CTO) 08-08 dtd 8 Nov 2008

(u) DoD Directive 8100.2, Use of Commercial Wireless Devices, Services and Technologies in the Department of Defense (DoD) Global Information Grid GIG), 14 Apr 2004

(v) DoD instruction 8510.01, Risk Management Framework (RMF) For DoD Information Technology (IT), 12 March 2014

APPENDIX (B)

OPNAV SECURITY SERVICED ACTIVITIES' UICs

The following UICs are reported under one UIC (65146) for personnel security clearances in JPAS under SMO 000114:

UIC	NAME	DATABASE
00011	Office of the Chief of Naval Operations	By Serviced Activity* (N097)
00166	Naval Air Facility, Andrews AFB (PNT Only)	N095
30320	Department of the Navy Information Technology Division	DON/AA ITD
30346	Board for Corrections Of Naval Records	BCNR
30571	Office of General Counsel	OGC
31572	Chief of Naval Personnel DET, Washington	N1
31698	Office of the Secretary of the Navy	SECNAV
31699	Office of the Under Secretary of the Navy	DON/AA
31701	Maritime Domain Awareness	DUSN
31703	Deputy Under Secretary of the Navy, Integrated Support Directorate	DUSN(P)/ISD
31705	Chief of Information Office	CHINFO
31921	Joint Interoperation Air Missile Defense Organization	JCS/J8
31975	Chief Information Officer	DON CIO
32039	COMNAVAIRFORCE DET Reserve Pay Navy	N98

32286	FLTCYB SPT	N2N6
32412	FLTCYB	
32790	Secretary of the Navy, Reserve Navy Activity	By Serviced Activity*
32791	Chief of Naval Operations Reserve Pay (PNT Only)	By Serviced Activity*
3342B	PERS RSCH	CNP (N15)
3344B	Bureau of Naval Personnel	N1
3420B	OGC Summer Interns/Law Clerks	OGC
34912	Counter-Narcotics (1 Person)	DUSN(P)
34913	Assistant Secretary of the Navy Drug Demand Reduction Program	ASNMRA
3495B	Chief of Naval Personnel (Pers-6 Washington Liaison DET)	N1
35058	Department of the Navy Staff Offices	By Serviced Activity*
3833A	Chief of Naval Personnel	N12/N13
41421	Office of the Deputy Comptroller	ASNFMC
42161	Undersea Enterprise (OPNAV LNO)	
42217	Office of the Assistant Secretary of the Navy, Manpower and Reserve Affairs	ASNMRA
42485	DON/Assistant Administration	DON/AA
43023	OPNAV Navy Command Center	N3N5
43116	ASNEIE Guam Program Office	ASNEIE
43380	FLTCYB UNSECNAV SUPPORT	
43440	Chief of Naval Personnel	N1

44802	ONI/N2 Check-in w/CNO (SSO)	N2N6
44860	DNI OPNAV Support Staff	N2N6
4577A	Chief of Naval Operations and Chief of Naval Personnel (has N1 billet and an N8 billet)	By Serviced Activity*
46699	Chief of Naval Education and Training (Personnel permanently Assigned to PNT)	N1
47039	Office of the Chief of Naval Operations	By Serviced Activity*
47218	Dep Under Secretary of the Navy	DUSN(P)
47315	Navy and Marine Corps Appellate Leave Activity	N1 (NAMALA)
47402	OPNAV JMCIS/GCCS	N3N5
47454	Commander Naval Reserve Force Staff DET (N095 PNT Employees Only)	N095
47691	Navy DMA Liaison Office, OIC	CHINFO
47891	MPTE Leadership and Management Support DET	N1
48142	Assistant Secretary of the Navy Research, Development and Acquisition	ASNRDA
48143	Assistant Secretary of the Navy Energy Installations and Environment	ASNEIE
48144	Office of the Under Secretary Of the Navy Support Center (TQM)	SECNAV (SAPRO)
32240	CNRC DET Arlington VA	
48145	Small and Disadvantaged Business Utilization	SECNAV
48146	Assistant Deputy Under	DUSN(M)

	Secretary of the Navy, Safety and Survivability		
48766	Naval Financial Management Career Center, NAS Pensacola		ASNFMC
49440	NAVSPECWARCOM DET		
49943	STU Legislative Affairs Fellows Program		OLA
62695	Naval Audit Service Headquarters		NAVAUD
62980	Commander Naval Reserve Force Staff DET	By Serviced Activity*	
63423	OPNAV DET Site "R"		N3N5
63959	Quarters Chief of Naval Operations (For military Personnel assigned to Flag Quarters in National Capital Region/PQMESS	By Service Activity* Realigned PQMESS to CNIC	
66032	DASN ENERGY		ASN(EI&E)
66123	Navy Department of Legislative Affairs		OLA
66760	Navy Public Affairs Office Navy Department Staff Offices		CHINFO
68027	Commerce Department (NOAA) (formerly N096, N7C Naval Observatory)		N2N6
68499	Navy Council of Review Boards		SECNAV CORB
68864	Naval Center for Cost Analysis (NCCA)		ASNFMC
68910	Legal Services Support Group		OGC
83852	Senior Executive Office for Manpower Personnel (4 billets)		N095

*Listing of valid Security Codes

N00	N8S	N99	NAVAUD
N09	N80	SECNAV	OGC
N09F	N81	DON/AA	OLA
N093	N83	DUSN(M)	SECNAVCORB
N095	N9	DUSN(P)	
N097	N9I	ASNEIE	
DNS	N9SP	ASNFMC	
N1	N94	ASNMRA	
N10	N95	ASNRDA	
N2N6	N96	BCNR	
N3N5	N97	CHINFO	
N4	N98	DON CIO	

The following UICs reported under one UIC (65146) for personnel security clearances in JPAS under SMO 000114:

UIC	NAME	DATABASE
00011	Office of the Chief of Naval Operations	By Serviced Activity* (N097)
00166	Naval Air Facility, Andrews AFB (PNT Only)	N095
30320	Department of the Navy Information Technology Division	DON/AA ITD
30346	Board for Corrections Of Naval Records	BCNR
30571	Office of General Counsel	OGC
31572	Chief of Naval Personnel DET, Washington	N1
31698	Office of the Secretary of the Navy	SECNAV
31699	Office of the Under Secretary of the Navy	DON/AA
31701	Maritime Domain Awareness	DUSN
31703	Deputy Under Secretary of the Navy, Integrated Support Directorate	DUSN(P)/ISD

31705	Chief of Information Office	CHINFO
31921	Joint Interoperation Air Missile Defense Organization	JCS/J8
31975	Chief Information Officer	DON CIO
32039	COMNAVAIRFORCE DET Reserve Pay Navy	N98
32240	CNRC DET Arlington, VA	
32286	FLTCYB SPT	N2N6
32412	FLTCYB	
32790	Secretary of the Navy, Reserve Navy Activity	By Serviced Activity*
32791	Chief of Naval Operations Reserve Pay (PNT Only)	By Serviced Activity*
3342B	PERS RSCH	CNP (N15)
3344B	Bureau of Naval Personnel	N1
3420B	OGC Summer Interns/Law Clerks	OGC
34912	Counter-Narcotics (1 Person)	DUSN(P)
34913	Assistant Secretary of the Navy Drug Demand Reduction Program	ASNMRA
3495B	Chief of Naval Personnel (Pers-6 Washington Liaison DET)	N1
35058	Department of the Navy Staff Offices	By Serviced Activity*
3833A	Chief of Naval Personnel	N12/N13
41421 42161	Office of the Deputy Comptroller Undersea Enterprise (OPNAV LNO)	ASNFMC
42217	Office of the Assistant	ASNMRA

	Secretary of the Navy, Manpower and Reserve Affairs	
42485	DON/Assistant Administration	DON/AA
43023	OPNAV Navy Command Center	N3N5
43116	ASNEIE Guam Program Office	ASNEIE
43380	FLTCYB UNSECNAV SUPPORT	
43440	Chief of Naval Personnel	N1
44802	ONI/N2 Check-in w/CNO (SSO)	N2N6
44860	DNI OPNAV Support Staff	N2N6
4577A	Chief of Naval Operations and Chief of Naval Personnel (has N1 billet and an N8 billet)	By Serviced Activity*
46699	Chief of Naval Education and Training (Personnel permanently Assigned to PNT)	N1
47039	Office of the Chief of Naval Operations	By Serviced Activity*
47218	Dep Under Secretary of the Navy	DUSN(P)
47315	Navy and Marine Corps Appellate Leave Activity	N1 (NAMALA)
47402	OPNAV JMCIS/GCCS	N3N5
47454	Commander Naval Reserve Force Staff DET (N095 PNT Employees Only)	N095
47691	Navy DMA Liaison Office, OIC	CHINFO
47891	MPTE Leadership and Management Support DET	N1
48142	Assistant Secretary of the Navy Research, Development and Acquisition	ASNRDA

48143	Assistant Secretary of the Navy Energy Installations and Environment		ASNEIE
48144	Office of the Under Secretary Of the Navy Support Center (TQM)	SECNAV	(SAPRO)
48145	Small and Disadvantaged Business Utilization		SECNAV
48146	Assistant Deputy Under Secretary of the Navy, Safety and Survivability		DUSN(M)
48766	Naval Financial Management Career Center, NAS Pensacola		ASNFMC
49440	NAVSPECWARCOM DET		
49943	STU Legislative Affairs Fellows Program		OLA
62695	Naval Audit Service	NAVAUD Headquarters	
62980	Commander Naval Reserve Force Staff DET	By Serviced Activity*	
63423	OPNAV DET Site “R”		N3N5
63959	Quarters Chief of Naval Operations (For military Personnel assigned to Flag Quarters in National Capital Region/PQMESS)	By Service Activity* Realigned PQMESS to CNIC	
66032	DASN ENERGY		ASN(EI&E)
66123	Navy Department of Legislative Affairs		OLA
66760	Navy Public Affairs Office Navy Department Staff Offices		CHINFO
68027	Commerce Department (NOAA) (formerly N096, N7C Naval Observatory)		N2N6
68499	Navy Council of Review Boards	SECNAV CORB	

68864	Naval Center for Cost Analysis (NCCA)	ASNFMC
68910	Legal Services Support Group	OGC
83852	Senior Executive Office for Manpower Personnel (4 billets)	N095

*Listing of valid Security Codes

N00	N8S	N99	NAVAUD
N09	N80	SECNAV	OGC
N09F	N81	DON/AA	OLA
N093	N83	DUSN(M)	SECNAVCORB
N095	N9	DUSN(P)	
N097	N9I	ASNEIE	
DNS	N9SP	ASNFMC	
N1	N94	ASNMRA	
N10	N95	ASNRDA	
N2N6	N96	BCNR	
N3N5	N97	CHINFO	
N4	N98	DON CIO	

APPENDIX (C)

FORMS

1. The following forms are available through DNS-34 or GSA Forms Library Web site: http://www.gsa.gov/portal/forms/type/TOP.

a. OF 7 Property Pass

b. OF 8 Position Description

c. SF 153 COMSEC Material Report

d. SF 311 Agency Security Classification Management Program Data

e. SF 312 Classified Information Nondisclosure Agreement

b. SF 701 Activity Security Checklist

g. SF 702 Security Container Check Sheet

2. The following SFs can be ordered through GSA with the appropriate stock number at www.gsaglobalsupply.gsa.gov or www.gsaadvantage.gov:

a. SF 87 Finger Print Chart Stock Number

b. SF 700 Security Container Information

c. SF 703 Top Secret (Coversheet)

d. SF 704 Secret (Coversheet)

e. SF 705 Confidential (Coversheet)

3. The following Department of Defense Forms (DD) can be downloaded from the DoD Forms Web site: http://www.esd.whs.mil/Directives/forms/

a. DD 254 Department of Defense Contract Security Classification Specification

b. DD 2056 Telephone Monitoring Notification Decal

c DD 2923 Privacy Act Data Cover

4. The following DD and OPNAV forms can be obtained either from Naval Forms Online: https://navalforms.documentservices.dla.mil/ or the OPNAV Security Office at the Pentagon, Room 4C659:

a. DD 2501 Courier Authorization

b. OPNAV 5216/4 Outgoing Mail Record

c OPNAV 5239/14 System Authorization Access Request Navy (SAAR-N)

d OPNAV 5239/15 Classified Hard Drive Destruction Log

e. OPNAV 5510/418 Security Indoctrination Certification and Request for Clearance and Special Accesses

f. OPNAV 5511/5 Security Violation Report

g. OPNAV 5511/10 Record of Receipt

h. OPNAV 5511/12 Classified Material Destruction Report

i. OPNAV 5511/13 Disclosure Record (available in Room 4C659)

j. OPNAV 5511/14 Security Termination Statement

5. The following forms are controlled and issued by Pentagon Force Protection Agency (PFPA):

a. DD 2249 DoD Building Pass Application

b. DD 2843 Classified Material Destruction Record

6. DOE HQ F 5631.20 Request For Visit or Access Approval is available online at DOE via: https://energy.gov/cio/downloads/doe-f-563120