



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

OPNAVINST 5511.35M
N3/N5
13 Jan 2016

OPNAV INSTRUCTION 5511.35M

From: Chief of Naval Operations

Subj: SAFEGUARDING NUCLEAR COMMAND AND CONTROL EXTREMELY
SENSITIVE INFORMATION

Ref: (a) CJCSI 3231.01B
(b) SECNAV M-5510.36, Department of the Navy
Information Security Program of January 2006
(c) SECNAV M-5510.30, Department of the Navy
Personnel Security Program of January 2006

Encl: (1) Safeguarding Nuclear Command and Control Extremely
Sensitive Information
(2) Procedures for Safeguarding NC2-ESI within the Office
of the Chief of Naval Operations
(3) Sample Request for Access to NC2-ESI Memo

1. Purpose. To implement reference (a), the Joint Chiefs of Staff (JCS) policy for safeguarding nuclear command and control (NC2) extremely sensitive information (ESI). Major changes to this revision include:

a. Minor policy changes, while verifying compliance and applicability with current references.

b. Removal of duplicative direction that is already contained in the parent references for ease of use.

c. Removal of social security number requirement when verifying security clearance, per Department of Defense (DoD) Instruction 1000.30 of 1 August 2012. This instruction is a substantial revision and should be read in its entirety.

2. Cancellation. OPNAVINST F5511.35L.

3. Scope and Applicability

a. This instruction applies to all U.S. Navy personnel holders, users, and processors of NC2-ESI, and material previously classified as Single Integrated Operations Plan-Extremely Sensitive Information (SIOP-ESI).

b. Reference (a) provides complete instructions from the Chairman of the Joint Chiefs of Staff (CJCS) for NC2-ESI. References (b) and (c) provide complete instructions for the Department of the Navy (DON) Personnel Security and Information Security Programs, respectively. They prescribe measures for accreditation, visitors, classification, reproduction, destruction, accountability, safekeeping, storage, transfer, transportation, dissemination, and transmission of official information, and include within their scope the documents that constitute NC2-ESI. This instruction is supplemental to references (a) through (c). It provides additional guidance to Navy commands where necessary and applies specifically to NC2-ESI.

c. Enclosures (1), (2), and (3) contain the policy and procedures for the DON with regard to the security of NC2-ESI. This instruction applies to all holders, users, and processors of NC2-ESI and material previously classified SIOP-ESI. Enclosure (3) is a sample memo and must contain all information indicated.

4. Background. Information regarding command and control of nuclear weapons is a high-level intelligence collection target. Disclosure of this information to unauthorized persons could result in serious degradation of the Nation's effectiveness and survivability in a nuclear exchange; disclosure would cause extremely grave damage to national security and therefore information regarding command and control of nuclear weapons should be designated NC2-ESI. The distribution of and access to NC2-ESI must be strictly limited; based on rigorously justified operational requirements and "need-to-know"; and must be protected under the provisions set forth in reference (a), this instruction, and enclosures (1) through (3).

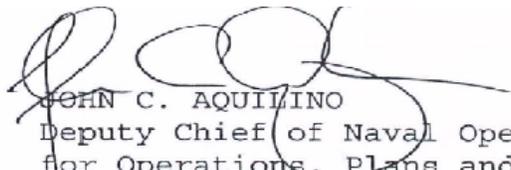
5. Action

a. All Navy commands and activities that have access to NC2-ESI materials and material previously classified as SIOP-ESI must comply with this instruction. Commands must safeguard these materials per references (a) through (c) in addition to implementing directives of appropriate commanders.

b. All Navy commands and activities that have access to NC2-ESI materials must designate an NC2-ESI control officer in writing.

c. Changes to this instruction may be recommended to Deputy Chief of Naval Operations for Operations, Plans, and Strategy, Nuclear Weapons Policy Branch (OPNAV (N514)) at (COMM) (703) 693-2775, (DSN) 223-2775.

6. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy (SECNAV) Manual 5210.1 of January 2012.


JOHN C. AQUILINO
Deputy Chief of Naval Operations
for Operations, Plans and
Strategy

Distribution:

Electronic only, via Department of the Navy Issuances Web site
<http://doni.documentservices.dla.mil>

SAFEGUARDING NUCLEAR COMMAND AND CONTROL EXTREMELY SENSITIVE
INFORMATION

1. Identification of NC2-ESI. The categories of NC2-ESI are specified in reference (a). It is emphasized that access to these categories must be strictly limited to those requiring the materials and information because it is essential to the performance of their duties.

2. Security Classification and Marking. All NC2-ESI material must be classified top secret and marked per reference (a).

3. Distribution and Reproduction of NC2-ESI Material and Extracts

a. The distribution and reproduction of NC2-ESI material and derivative information must be per reference (a).

b. The Chief of Naval Operations (CNO) will advise the CJCS prior to the Chairman, and provide a recommendation to the Secretary of Defense to approve or disapprove Congressional requests for NC2-ESI documents.

c. The CNO will endorse any Navy-originated request to release NC2-ESI material to foreign nationals before the request is submitted to Commander, U.S. Strategic Command (USSTRATCOM). The CNO will advise the CJCS regarding release of NC2-ESI material to foreign nationals prior to the Chairman's recommendation to the Secretary of Defense. When approved, reproduction and attendant accountability must be per reference (a).

d. Recipients of NC2-ESI must comply with reference (a) when processing receipt. Commands unable to comply within 72 hours due to communications difficulties, electronic silence procedures, or other impediments unique to ships at sea must inform their immediate superior in command and report receipt of documents as soon as possible.

4. Inventory and Sighting

a. NC2-ESI materials must be inventoried, controlled, and destroyed per reference (a).

b. Per reference (a), NC2-ESI materials must be destroyed within 30 days of supersession. When DON originated exceptions to this requirement are unable to be met, they must be endorsed by the Deputy Chief of Naval Operations for Operations, Plans and Strategy (CNO (N3/N5)) prior to submission to Joint Staff Deputy Director for Global Operations for the Executive Branch, or USSTRATCOM Director, Global Operations (USSTRATCOM J3).

5. Access Control

a. The command NC2-ESI control officer must maintain the NC2-ESI access list, per reference (a). Requests for access to NC2-ESI materials will follow the sample in enclosure (3).

b. Access to NC2-ESI materials must be per reference (a).

c. Waivers for permanent access and temporary access may be granted per reference (a).

d. All contractor requests, per reference (a), must be submitted to the appropriate office via OPNAV (N51). Allow a minimum of 15 working days to process contractor access requests.

e. Requests not covered in subparagraphs 5f(1) through 5f(9) will be submitted to OPNAV (N51) for approval.

f. The DON directorates and commands in subparagraphs 5f(1) through 5f(9) may delegate authority to establish billets and grant access to NC2-ESI material.

(1) Office of Chief of Naval Operations Director, Strategy and Policy Division (OPNAV (N51)) for all military and DoD civilian personnel within the OPNAV staff, and for military and DoD civilian personnel assigned to the offices of the SECNAV.

(2) Director, Strategic Systems Programs for all DoD civilians and military personnel supporting his or her command.

(3) Commander, Submarine Forces; Commander, Submarine Force Atlantic; and Commander, Submarine Force, U.S. Pacific Fleet for military and DoD civilian members of his or her staffs, and subordinate group and squadron commanders requiring

NC2-ESI access. Ship, nuclear powered ballistic-missile (SSBN), command and control inspection personnel will not normally require access due to the use of training materials vice actual NC2 documents during inspections.

(4) Group and or squadron commanders for military and DoD civilian members of his or her staffs requiring NC2-ESI access and all subordinate SSBN commanding officers. Limit personnel access to NC2-ESI Category C to those requiring unescorted access to Commander U.S. Strategic Command Emergency Action Procedures (EAP-STRAT) Volume 2.

(5) SSBN commanding officers for subordinate military crew members requiring NC2-ESI access. Limit access to NC2-ESI Category C to the executive officer, operations officer, and officers functioning as emergency action team members and radio room watchstanders who require unescorted access to EAP-STRAT Volume 2.

(6) Commander, Strategic Communications Wing ONE (COMSTRATCOMMWING ONE) for military and DoD civilian members of his or her staff requiring NC2-ESI access.

(7) COMSTRATCOMMWING ONE squadron commanding officers for subordinate military personnel requiring NC2-ESI access. The minimum personnel that require NC2-ESI Category B and C access are all naval flight officers, including combat systems officers, combat system officer trainees, and airborne communications officers who require unescorted access to view the Emergency Action Procedures of the Chairman of the Joint Chiefs of Staff (EAP-CJCS) Volume IV and EAP-CJCS Volume II. All other E-6B aircrew positions require Category E access due to incidental exposure to NC2-ESI materials and information in the performance of their duties. The minimum personnel that require NC2-ESI Category C and D access are selected communications and intelligence personnel who utilize NC2-ESI information.

6. Actions Following Possible or Actual Compromise. Perform the actions required in references (a) and (b). Inform CNO (N3/N5) by the most expeditious means available.

7. Information System Media

a. Recording media used to store or process NC2-ESI must retain the top secret classification and be controlled as NC2-ESI until declassification procedures delineated in reference (a) are carried out.

b. Policies and procedures for the security of NC2-ESI information processed, communicated, or stored are discussed in reference (a).

PROCEDURES FOR SAFEGUARDING NC2-ESI WITHIN THE
OFFICE OF THE CHIEF OF NAVAL OPERATIONS

1. Purpose. To establish supplemental procedures for the processing and safeguarding of NC2-ESI within the SECNAV and OPNAV staff.
2. General. The responsibility for developing and issuing CNO policy for safeguarding NC2-ESI and maintaining access to NC2-ESI materials resides with OPNAV (N51). An OPNAV NC2-ESI control officer from OPNAV (N51) must be assigned the responsibility for maintaining the SECNAV and OPNAV NC2-ESI access list per reference (a).
3. Information Control Procedures
 - a. All NC2-ESI materials and messages must be received, distributed, and maintained by the OPNAV NC2-ESI control officer. NC2-ESI documents must be returned to the OPNAV NC2-ESI control officer when no longer required.
 - b. All NC2-ESI materials must be controlled from receipt to destruction using the procedures in reference (b).
4. Personnel Access Control
 - a. Categories of NC2-ESI are described in reference (a). Access to these categories must be strictly limited to those requiring the materials and information because it is essential to the performance of their duties.
 - b. The OPNAV NC2-ESI control officer must maintain a list of billets requiring permanent access. The list must be reviewed and validated annually for accuracy.
 - c. Requests for NC2-ESI access must be forwarded to the OPNAV NC2-ESI control officer for processing. Temporary access will normally be granted up to 1 year.
 - d. This enclosure must be used to ensure all personnel granted access meet the access criteria of reference (a). A briefing certificate must then be executed per reference (a).

OPNAVINST 5511.35M
13 Jan 2016

e. The OPNAV NC2-ESI control officer must retain the original access requests for 2 years after debriefing of personnel, as well as an access roster for all SECNAV and OPNAV personnel that are authorized access to NC2-ESI.

f. When staff members are detached or otherwise transferred, they must contact the control officer who will execute the debriefing statement.

SAMPLE REQUEST FOR ACCESS TO NC2-ESI MEMO

From: LCDR D. O. Good, NC2-ESI Control Officer
To: Approving Official

Subj: REQUEST FOR ACCESS TO NC2-ESI

Ref: (a) OPNAVINST 5511.35M

1. It is requested that the following individual, certified to have a "need to know" per reference (a), be granted access to NC2-ESI for the categories listed below:

Name (Last, First MI)	Rank/GS	DODID	Billet	*Cat*
Date of Birth:		Place of Birth:		

Signature Date

FIRST ENDORSEMENT

From: Command Security Manager
To: Approving Official

1. The above named applicant is certified to possess a FINAL TOP SECRET clearance. An SSBI or periodic reinvestigation has been initiated and completed as indicated below.

SSBI/PR initiated on:	
SSBI/PR completed on:	
SSBI/PR completed by:	

Signature Date

SECOND ENDORSEMENT

From: Approving Official

1. Access to NC2-ESI information is granted/not granted (circle one).

Signature Date

FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.
AUTHORITY: 5 U.S.C. 9101; 10 U.S.C. 137; DoD Directive 1145.02E; DoD 5200.2R; DoD 5105.21; DoD Instruction (DoDI) 1304.26; DoDI 5200.02; DoDD 5220.6; DoDI 5220.22; Homeland Security Presidential Directive (HSPD) 12; and E.O. 9397 (SSN), as amended; DMDC 12 DoD <http://dpcld.defense.gov/Privacy/SORNSIndex/DODwideSORNArticleView/tabid/6797/Article/570567/dmdc-12-dod.aspx>
Additional authorities: OPNAV INST 5511.35M Safeguarding Nuclear Command and Control Extremely Sensitive Information (NC2-ESI)
PURPOSE: To verify the security clearance classification of the personnel that is requesting access to NC2-ESI.
ROUTINE USES: Data is used by OPNAV NC2-ESI Control Officer, who has a need to know in order to process requests for access.
DISCLOSURE: Voluntary; however, failure to provide the requested information may result in a delay or inability to process requests.