OPNAVINST N9210.3
7 Jun 2010

# SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION (NNPI)

## UNCLASSIFIED PORTION (OMITS TABLE 2)

## RECORD OF CHANGES

| IDENTIFICATION OF CORRECTION OR CHANGE | DATE OF CHANGE | DATE OF ENTRY | ENTERED BY |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

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

OPNAVINST N9210.3
N00N
7 Jun 2010

OPNAV INSTRUCTION N9210.3

From: Chief of Naval Operations

Subj: SAFEGUARDING OF NAVAL NUCLEAR PROPULSION INFORMATION

1. Purpose. This instruction defines naval nuclear propulsion information (NNPI) and establishes the safeguarding policies and requirements for such information.

2. Cancellation. NAVSEAINST 5511.32C.

3. Applicability and Scope

a. The provisions of this instruction are applicable to all equipment, components, systems, documents, drawings, information technology (IT) media, audiovisual media, and any other media or items containing classified or unclassified NNPI.

b. This instruction applies to all Navy commands and to all military and civilian personnel assigned to or employed by any element of the Navy that handles or processes classified or unclassified NNPI. This includes cleared contractor visitors working under the purview of a commanding officer (CO). Personnel are individually responsible for compliance.

c. This instruction applies to all Navy activities, organizations, and contractors who: (1) use Navy information systems that receive, process, store, display, or transmit classified or unclassified NNPI; or (2) operate systems on behalf of the Navy or own facilities or systems that process classified or unclassified NNPI associated with Navy contracts.

4. Background. The policies and requirements previously set forth in NAVSEAINST 5511.32C have been updated and restructured into this instruction, which should be reviewed in its entirety.

5. Implementation

a. Navy activities that handle or processes NNPI shall advise Director, Naval Nuclear Propulsion Program (CNO (N00N))

within 60 days of the date of this letter of any reason preventing implementation of this instruction and the date by which all provisions of this instruction will be met.

b. Supervisors of Shipbuilding, Conversion, and Repair (SUPSHIPs) should issue a field modification request to private shipyards to incorporate this instruction into existing contracts and into the VIRGINIA-class master index of reference documents whenever possible at no increase in contract price or delay in delivery. If implementing this instruction will increase the price of or delay delivery under any contract, then this instruction should not be implemented without authorization from CNO (N00N). In such cases, the respective SUPSHIP should obtain a fully priced proposal to implement this instruction on existing contracts. CNO (N00N) should be advised within 60 days of the date of this instruction whether this instruction has been implemented, and if not, a date by which implementation will be completed.

6. Action. Navy activities shall implement the guidance contained herein and all associated references. All Navy activities handling/processing NNPI or otherwise involved in the safeguarding of NNPI shall budget for, fund, and execute the actions necessary to comply with this instruction and the publications that support it.

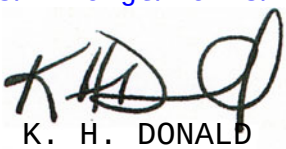
7. Administration and maintenance. CNO (N00N) shall ensure implementation of the provisions of this instruction, grant any exceptions needed, and address inquiries concerning the requirements contained herein. CNO (N00N) may also provide direction and guidance under its other organizational designations of “Naval Sea Systems Command” or “Naval Reactors.”

8. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy (SECNAV) Manual (M-)5210.1 of November 2007.

9. Forms

a. OPNAV 9210/1 IT Checklist for NNPI can be obtained from Naval Forms Online at <http://navalforms.daps.dla.mil>.

b. DD 254 DoD Contract Security Classification Specification can be obtained from the DoD Forms Web site at <http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm>.



K. H. DONALD
Director, Naval Nuclear
Propulsion Program

Distribution: Electronic only

Department of the Navy Issuances Web site - Unclassified portion (omits table 2): <http://doni.daps.dla.mil>

Secret Internet protocol router network (SIPRNET) Department of the Navy Classified Issuances Web site - Complete instruction: <http://hqweb.cno.navy.smil.mil/donci>

# TABLE OF CONTENTS

## TABLE OF CONTENTS (CONT'D)

## TABLE OF CONTENTS (CONT'D)

## TABLE OF CONTENTS (CONT'D)

## TABLE OF CONTENTS (CONT'D)

**TABLE 3 (CONT'D) IT CONTROL REQUIREMENTS FOR NNPI (CONT'D)**



**EXHIBITS**

# CHAPTER 1
# DEFINITION

1. Definition. NNPI is classified or unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.

2. Guidance

a. Table 1 and exhibit 1 discuss the different classification levels/handling controls for NNPI.

b. Table 2 identifies those specific systems and components associated with naval nuclear propulsion plants and the nuclear support facilities.

3. NNPI Determination

a. NNPI shall be safeguarded to prevent its disclosure to the public and others without the appropriate clearance (for classified NNPI) and a need-to-know (NTK). This section describes the process for identifying if an item is NNPI.

b. Whenever a sentence, paragraph, document, file, photograph, audiovisual or electronic/IT media, or component contains, or otherwise reveals, at least one instance of an association of the following three elements, it is NNPI:

(1) A naval nuclear propulsion plant or support facility application is directly referred to by any of the following:

(a) Ship name or hull number.

(b) Project designator.

(c) Ship system identification.

(d) Component nameplate data.

(e) Component name revealing a reactor plant function.

(2) A system or component listed in table 2.

(3) Details on technical parameters or operational conditions (e.g., design temperature or pressure).

c. Items or information specifically identified by CNO (N00N) as NNPI shall be marked and handled as such.

d. For systems listed in table 2 that have an asterisk [*] in the category column, the information on components, equipment, and subsystems installed in these systems may also be NNPI. An instance of the association of such information with both the elements in subparagraphs 3b(1) and 3b(3) above is NNPI unless one of the following applies for the component/equipment/subsystem (Note: the exhibit 2 flow chart may assist with evaluation):

(1) It is available “commercial off-the-shelf.”

(2) It is an individual piece part (fastener, handwheel, gasket, packing, valve stem, etc.) or electrical part (resistors, capacitors, semiconductors, switches, relays, contactors, etc.). This includes piece parts whose label plates list system designations (e.g., valve or component system numbers) or manufacturers’ general component information plates. This applies to individual piece parts even if the component assembled from them is a classified or sensitive reactor plant component.

(3) It is military-qualified and used in (or is technically equivalent to a military-qualified component used in) Navy applications other than naval nuclear applications (ship system valves, circuit boards, circuit breakers, controllers, etc.).

(4) It meets other exemption criteria as determined by CNO (N00N).

4. Classification/Handling Control Determination. If the subparagraphs 3b through 3d evaluation identifies information as NNPI, the classifications of Confidential Restricted Data (CRD), Confidential National Security Information (CNSI), or another classified marking or handling control is determined by requirements set forth in references (a) and (b). Reference (a)

also includes guidance for the determination of unclassified naval nuclear propulsion information (U-NNPI), unclassified controlled nuclear information (UCNI), or unrestricted unclassified information. If the subparagraphs 3b through 3d evaluation identifies information as NNPI, but classification or handling controls are not otherwise prescribed per references (a) and (b), then the item shall be marked and handled as U-NNPI.

5. Information on Supporting Technologies. Technology (including basic research, test data, evaluation methods, and behavior models) developed to support applications unique to the Naval Nuclear Propulsion Program (NNPP), whether the information is NNPI or not, should be considered proprietary information not releasable to the public until determined otherwise by CNO (N00N).

# CHAPTER 2
# MARKING

1. General. Chapter 2 establishes marking requirements for NNPI. Special handling and disclosure restrictions for NNPI have been in effect since the NNPP's inception. Prior to 1986, the large majority of unclassified documents were not marked with special warning notices. With the enactment of Federal statutes mandating protective measures for a range of sensitive military technology, including NNPI, marking became necessary. Whoever possesses NNPI must comply with the disclosure restrictions set forth in this instruction, whether or not the documents, media, or equipment containing NNPI are marked with a warning notice.

2. NNPI Control Officer (NNPICO). Each activity that routinely deals with NNPI shall designate a manager familiar with NNPI protection procedures as NNPICO. Each activity will ensure that this manager is technically qualified or a technically qualified individual is available for consultation with the NNPICO as needed. It shall be this manager's responsibility to ensure that appropriate measures are established and enforced to control, and to prevent unauthorized access to or dissemination of, NNPI per this instruction. This individual will be given written authorization by the cognizant Government office/CO to determine if documents are correctly marked as NNPI (without review by CNO (N00N)).

3. Prospective Marking Requirement. All documents containing NNPI issued subsequent to the date of this instruction shall be marked following this instruction. Applicable local instructions should address requirements for marking of electronic documents, including email. Documents marked per past versions of this instruction do not require any modification. When portions of unmarked documents are revised or replaced, those portions and the cover, index, and distribution pages shall be marked following this instruction. When an unmarked document is reissued in its entirety, all pages shall be marked per this instruction. An older, unmarked document containing U-NNPI need not be marked if it is simply being copied for internal use and not for reissuance. Before offsite release of unmarked documents, they shall be marked and handled per this instruction.

4. Markings and Distribution Statements. References (a) and (b) contain classification and downgrading or declassification markings for classified NNPI. Exhibit 3 summarizes the marking and distribution statement requirements for NNPI. Exhibits 4, 5, and 6 provide sample NNPI documents with the appropriate markings and distribution warning statements for Not Releasable to Foreign Nationals (NOFORN), CRD, and CNSI, respectively.

5. Paragraph and Portion Markings. Paragraph or portion markings are not required for NNPI.

6. Photographs and Audiovisual Material. Photographs and audiovisual material will be marked consistent with the classification of the information therein. Photographs of naval nuclear-powered ships or nuclear support facilities shall be handled per reference (c). Audiovisual material containing NNPI shall be marked on the cover and case of each item, and at the beginning and end of each tape or reel.

7. IT Media, Equipment, and Electronic Display. IT media, equipment, and electronic display must be marked to identify the highest level of NNPI authorized. Per the Department of Defense (DoD) classification color scheme, the background color for IT media and equipment labels for classified NNPI should be red for SECRET, blue for CONFIDENTIAL, and green for U-NNPI. The foreground color for IT media and equipment labels should be white. The similar color scheme used for electronic display is discussed in subparagraph 7c.

a. IT media

(1) Classified NNPI IT media shall be marked by a pen/marker or using a media label with the appropriate classification level and shall include the proper distribution warning statement(s) from exhibit 3, where space permits.

(2) U-NNPI IT media shall be marked “NOFORN (U-NNPI)” either with an indelible pen or with a media label and shall include the NOFORN distribution warning statement from exhibit 3, where space permits.

(3) In those cases where the size or type of media does permit the use of classification/NOFORN (U-NNPI) markings, the

media shall be placed in a container marked with the appropriate level (including the appropriate distribution warning statement(s) from exhibit 3).

b. IT equipment. User-accessible NNPI IT equipment--such as printers, multifunction devices, desktops, laptops, mobile devices, and external hard drives--shall be labeled. NNPI hard drives, regardless of whether they are internal or external, shall be labeled. Activities should consider operational security when labeling portable user IT devices to avoid drawing attention to the device as a target for theft. For monitors and other display equipment with only volatile memory--a title bar, as discussed in subparagraph 7c below, may be used in place of a label.

(1) U-NNPI IT equipment.

(a) U-NNPI IT equipment shall be labeled "NOFORN (U-NNPI)" or "Approved up to Unclassified NNPI." The label should include the NOFORN distribution warning statement from exhibit 3, where space permits.

(b) IT equipment used to print U-NNPI (e.g. printers, facsimile (fax) machines, copiers, multifunction devices) shall also have a label, sign, or notice, including the appropriate user notice statement from exhibit 7. The label, sign, or notice shall be positioned on or near the IT equipment so as to be clearly visible to a user of the IT equipment.

(2) Classified NNPI IT equipment.

(a) Classified NNPI IT equipment shall have a label that identifies the highest classification authorized for the equipment. For CONFIDENTIAL- and SECRET-level IT equipment, the label shall include the proper distribution warning statement(s) from exhibit 3, where space permits.

(b) Classified NNPI IT equipment used to print NNPI (e.g., printers, fax machines, copiers, multifunction devices) shall also have a label, sign, or notice including the appropriate user notice statement from exhibit 7. The label, sign, or notice shall be positioned on or near the IT equipment so as to be clearly visible to a user of the IT equipment.

c. Electronic display

(1) Required markings for the electronic display of NNPI files, emails, application/Webpage content, and other IT elements are specified in exhibit 7. Note: Printed files, emails, and application/Webpage content shall adhere to requirements for marking hard copy NNPI documents per this chapter and exhibit 3.

(2) Monitors and display equipment used for NNPI-authorized IT equipment shall have a title bar on the screen identifying authorization for NNPI.

(a) This title bar must be continuously visible during use of the monitor with an NNPI-authorized IT system or piece of equipment, must be located at the top of the screen of a monitor, and include the appropriate user notice statement for NNPI from exhibit 7.

(b) The background color of the title bar should follow the DoD color scheme and set for the highest level of information authorized: red for up to SECRET, blue for up to CONFIDENTIAL, and green for up to U-NNPI. The foreground color for the text of the title bar should be white.

(c) Mobile devices approved for NNPI shall have the appropriate title bar to the maximum extent practical.

# CHAPTER 3
# CONTROL AND STORAGE

1. General. Classified NNPI shall be controlled per reference (b). U-NNPI shall be controlled so that those without an NTK cannot obtain visual or physical access that would permit detailed examination. U-NNPI documents are the custody of the authorized individual using them. This individual must prevent detailed visual or physical access by those who do not have an NTK. Whenever unauthorized personnel could gain access to U-NNPI, it should be locked up (e.g., key lock).

2. Transmittal. Classified NNPI will be transmitted per reference (b). Documents containing U-NNPI shall be transmitted in a single opaque envelope or wrapping, as a minimum. The envelope or wrapping shall not be marked so as to reveal its contents to unauthorized personnel.

3. Offsite Handling. U-NNPI may be taken offsite, subject to local controls approved by the cognizant Government office, which shall ensure that the U-NNPI is protected under the disclosure requirements of this instruction and that the U-NNPI is promptly returned when no longer needed offsite.

4. Facility Visits. Requirements for visits to naval and commercial facilities performing naval nuclear propulsion work are addressed in chapter 8. Additional guidance may also be found in reference (d).

5. Electronic Processing. Protection requirements for NNPI on IT systems, which for this instruction include telecommunication systems and other electronic equipment, are addressed in chapters 9 through 13. The protection requirements for IT media containing NNPI are addressed in chapters 2, 6, 9 and table 3.

# CHAPTER 4
# DISCLOSURE POLICY

1. General. Access to classified NNPI shall be limited only to those individuals with an NTK and an appropriate security clearance. For classified NNPI that is also restricted data (RD), a final Government clearance is required for access. Access to U-NNPI requires an NTK (as determined by local cognizant authority) for the performance of assigned work. CNO (N00N) must approve in writing any exception to this policy. Any changes in access policy from past actions should be identified to CNO (N00N). Additional specific disclosure policies are discussed below.

2. Foreign Disclosure. Reference (e) prohibits release of NNPI to foreign nationals or representatives of foreign interests except as made pursuant to an approved government-to-government agreement. Furthermore, releases to be made under such an agreement require approval from the Chief of Naval Operations (CNO) in each instance.

3. Dual Citizenship. All those with dual citizenship having a need to access U-NNPI must be reported to CNO (N00N) before such access is granted.

4. U.S. Executive Branch Personnel. Disclosure of NNPI to personnel in the executive branch of the U.S. Government, except for those involved in the NNPP, requires the approval of CNO (N00N) in each instance. The fact that an individual is employed by a U.S. Government activity does not in itself justify release of NNPI to that individual.

5. Outside the U.S. Government. Disclosure of NNPI outside the U.S. Government, including U.S. industry, private individuals, or other interests, except when required in the performance of NNPP tasks, requires CNO (N00N) approval in each instance.

6. Judicial or Administrative Proceedings. When access to NNPI is solicited as part of a judicial or administrative proceeding, CNO (N00N) shall be apprised via Naval Sea System Command (NAVSEASYSCOM) Office of Counsel (00L) to ensure that proper protective mechanisms are put in place to prevent unauthorized disclosure. These mechanisms may include formal protective orders or legal filings, and may result in denial of access.

7. Contractors and Subcontractors. These requirements are addressed in chapter 7.

8. Unauthorized Release. Any release of NNPI in violation of the disclosure policy outlined in this chapter shall be reported to CNO (N00N).

# CHAPTER 5
# PUBLIC RELEASE

1. General. NNPI shall not be disclosed in any manner that may result in direct or indirect release to the public. No public comment should be made that would confirm or deny whether NNPI has been inadvertently released to the public. Information released to the public is considered foreign disclosure. Any proposed public release that might contain NNPI must be submitted to CNO (N00N) via NAVSEASYSCOM Corporate Communications (00D) per reference (c). CNO (N00N) will authorize release of the information once it has been determined that it contains no NNPI.

2. Documents Containing NNPI. Use of NNPI in documents that are planned for release to the public is prohibited. The NNPI content shall be issued in a separate supplemental document to maintain control of NNPI. Also, references to documents containing NNPI in journals and other publications available to foreign governments or to the public should be avoided.

3. Environmental and Occupational Safety and Health (OSH) Information. Neither environmental information nor OSH information is NNPI unless presented in such a way that it reveals information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities. To the maximum extent practical, individuals should not include NNPI in documents that pertain to environmental or OSH matters since such documents are more likely to require public release.

# CHAPTER 6
# DISPOSAL

1. Documents

a. Disposal. NNPI documents shall be disposed as classified material.

b. Recycling of U-NNPI Documents. Recycling is authorized for U-NNPI documents provided that the documents are shredded to 1/2 inch width or less and that the shredded material is controlled in collection and transport to the recycler and controlled throughout the recycling process until such point in their processing that the U-NNPI documents are irretrievable.

c. Alternative Disposal or Recycling Methods. Alternative disposal or recycling methods (e.g. commercial or public trash collection arrangements) must be approved by CNO (N00N).

2. Components and Equipment

a. Before disposal of components or equipment that reveal NNPI, all markings (e.g., stock number, nameplate data, special material identification code (SMIC), tags, stickers, transfer documents, and meter face markings) associating the equipment or component with a nuclear propulsion plant application must be removed or obliterated. If after removal or obliteration of such markings the equipment or component would still reveal NNPI, the item shall be disposed of in the same manner as classified material.

b. In view of stringent controls for the disposal of radioactive waste, and in order to minimize radiological work, nuclear propulsion plant components or equipment to be disposed of as radioactive waste need not have markings removed or obliterated.

c. Unless specifically authorized by a ship alteration or other NAVSEASYSCOM correspondence, reactor plant components assigned 2S cognizance, SMIC X1 national stock numbers, shall not be disposed of unless first sent, per reference (f), to a designated naval shipyard for disposition by CNO (N00N). When

CNO (N00N) desires to dispose of such a component, a formal scrap directive will be provided to the naval shipyard awaiting disposition.

d. CNO (N00N Resource Management Division (H)) cognizance-, Naval Inventory Control Point (NAVICP)-managed SMIC X2, X3, X4, X5 or X6 material will be sent to NAVICP DOE Naval Reactors Material Office (Code 009) for disposal as directed by the NAVICP item manager. NAVICP (Code 009) will dispose of this material following NAVICP Naval Reactors Supply Chain Management Directorate (Code 87) instructions. However, selected CNO (N00N-H) cognizance SMIC X3 material items (e.g., resistors, capacitors, and handtools), which are not procured to nuclear-unique specifications, and other items designated by CNO (N00N) may be disposed of locally as directed by NAVICP (Code 87). Further, NAVICP-managed, CNO (N00N-H) cognizance SMIC X2 chemicals and other SMIC X2 materials may be disposed by naval shipyards, as directed by NAVICP (Code 87).

e. Disposition of unused, but no longer required, reactor plant equipment and components provided by CNO (N00N) prime contractors as Government-furnished equipment shall be per this instruction, reference (f), and specific guidance obtained from the NAVSEASYSCOM technical representative or assistant NAVSEASYSCOM technical representative at the applicable prime contractor.

f. Disposal of shipyard facilities, support systems, and equipment used in reactor plant work shall meet the criteria for disposal in subparagraphs 2a and 2b of this chapter.

3. Disposal of IT Equipment and Media. Special handling is required for disposal of IT equipment and media that contain NNPI. All non-volatile user-addressable memory materials must be removed from computing equipment ever used to process NNPI. This includes, but is not limited to, computer hard drive platters; removable media such as floppy disks, digital video disks (DVDs), compact disks (CDs), universal serial bus (USB) thumb-drives, and solid-state memory or hard drives; and programmable read-only memory (PROM) (including electronic storage devices embedded in multifunction equipment, such as copiers or printers). Note: this also applies to such materials involved in the unauthorized disclosures, spill, or inadvertent disclosure of NNPI.

a. U-NNPI materials shall be purged or destroyed per reference (g) before disposal or release outside of the NNPP. Disposal of U-NNPI as classified material is also acceptable.

b. Classified NNPI materials must be disposed of under National Security Agency (NSA) requirements for classified material.

# CHAPTER 7
# CONTRACTORS AND SUBCONTRACTORS

1. General. Requirements to protect NNPI shall be incorporated only into those contracts having a direct association with a naval nuclear propulsion plant application. When no such association exists, the contract does not involve access to NNPI and should not include contractual stipulations for its protection.

2. Contracted Goods and Services. Activities that procure material, components, or services involving access to NNPI shall ensure that appropriate requirements to control and protect NNPI are included in any such contracts or subcontracts.

3. Prospective Contractor. When providing a specification, drawing, or other technical document containing U-NNPI to a prospective contractor for the purposes of soliciting bids, the contracting activity shall use a stipulation to obtain prospective contractor agreement to control or protect the U-NNPI until subsequent contractual controls are established. Appendix C is a sample stipulation.

4. Classified NNPI. Contracts or subcontracts involving classified NNPI must incorporate all NNPI handling requirements into the DD-254 Department of Defense Contract Security Classification Specification of the contract or subcontract.

5. NN-801, NN-802, NN-817. Contractors or subcontractors obligated under existing contracts to adhere to the guidelines of NN-801 (Guidelines for the Control and Protection of Unclassified Naval Nuclear Propulsion Information), NN-802 (Guidelines for the Control and Protection of Classified Naval Nuclear Propulsion Information), or NN-817 (Naval Nuclear Propulsion Information Guide) shall continue to use those guidelines for protection of NNPI.

# CHAPTER 8
# FACILITY VISITS

1. General. Visits to naval and commercial facilities performing naval nuclear propulsion work present unique security problems due to the need to protect both unclassified and classified NNPI from unauthorized access or release. In particular, the scope and complexity of the repair, overhaul, and construction of U.S. Navy nuclear-powered ships are not always compatible with standard security and control measures. Access to NNPI is controlled principally by identifying and isolating areas within the facility that reveal NNPI. The security program necessary to protect NNPI will depend on the type of work being performed and the personnel access control procedures in effect. In all cases, however, local activity or facility heads are responsible for establishing a security program which will ensure compliance with the disclosure policy of this instruction.

2. U.S. Citizens and U.S. Nationals. Reference (b) and the security provisions of applicable Government contracts outline the required conditions, procedures, and responsibilities for visit approval.

3. Foreign Nationals or Representatives of a Foreign Interest

a. References (b) and (e) and the security provisions of applicable Government contracts apply. In addition, visits by foreign nationals or representatives of a foreign interest, whether for classified or unclassified purposes, require the specific approval of CNO (N00N) or designated representatives. Approval shall be obtained before the issuance of invitations or other commitments in order to protect NNPI and avoid unnecessary difficulties arising from denial of access. Requests for approval should contain activity plans for satisfying the special conditions outlined below. If all of these conditions cannot be satisfied, the visit shall either be diverted to an activity not engaged in naval nuclear propulsion work or be disapproved.

(1) The visitor(s) shall be kept under close and continuous surveillance at all times while within the physical confines of the facility.

(2) Visual, oral, and documentary disclosures of NNPI shall be prevented by isolating areas, materials, or personnel.

(3) The visit shall be accomplished without adverse impact on the facility's workload, scheduling, or other key management factors.

b. The special considerations above for visits by a foreign national or representative of a foreign interest are not required for those personnel continually performing custodial, maintenance, or administrative work that does not involve access to NNPI. In addition, in some instances, foreign nationals or representatives of foreign interests may be able to gain access to or near facilities--specifically, those that perform other diverse functions in addition to naval nuclear work--without being subject to formal access approval. In such cases, the activity is responsible for precluding unauthorized disclosure of NNPI, primarily through isolating areas or material that may reveal NNPI and carefully controlling the movement of these personnel at the activity.

c. Per the requirements of reference (e), foreign nationals or representatives of a foreign interest shall not be permitted access to the propulsion plant spaces of Navy nuclear-powered warships without the specific approval of the CNO.

# CHAPTER 9
# INFORMATION TECHNOLOGY (IT) POLICY

1. General. For this instruction, IT is an umbrella term that includes all technologies used for the processing of information, including telecommunication systems and other electronic equipment. Previous chapters discussed the control and protection of components, documents, photographs, or audiovisual material that contain NNPI. This chapter discusses the general policy for the control and protection of NNPI on IT systems. Additional requirements for NNPI on the three specific types of IT are discussed in subsequent chapters. For the purposes of this instruction, the three types of IT are:

a. Information Systems (discussed in chapter 11). Consist of any Navy information system that, per reference (h), is certified and accredited by the Navy designated accrediting authority (DAA) or designated as platform information technology (PIT) by the DAA.

b. Telecommunication Systems (discussed in chapter 12). Consist of voice, fax, or video communications equipment that may be networked but are distinct from information systems.

c. Other Electronics (discussed in chapter 13). Consist of electronics such as copiers and other standalone electronics distinct from and not otherwise addressed as part of information systems or telecommunication systems.

2. Requirements. NNPI shall be safeguarded on IT systems.

a. Safeguards shall be applied such that NNPI is (1) accessed only by authorized individuals, (2) processed only on authorized IT systems, (3) processed only within authorized workspaces or environments, (4) used only for its authorized purpose(s), and (5) properly handled, marked, labeled, and disposed.

b. NNPI shall be safeguarded on IT systems by implementing a coordinated set of operational, managerial, and technical security controls. Table 3 and its associated form, OPNAV 9210/1 IT Checklist for NNPI, provide requirements for IT systems and IT media regarding control and protection for NNPI.

c. IT systems used for NNPI should be marked/labeled following chapter 2 specifications for IT equipment, IT media, and electronic display.

d. NNPP activities shall adhere to requirements and guidance of the proper IT governing organization, including references (h) through (p). Conflicts involving NNPI and other IT requirements shall be resolved by the DAA (or governing authority) and CNO (N00N).

e. Responsibilities for implementing, controlling, and protecting NNPI on IT systems are assigned in chapter 10.

3. Restrictions

a. NNPI may only be authorized for IT systems owned or operated by, for, or on behalf of an NNPP activity.

b. IT systems located outside the United States or its territories require specific approval from CNO (N00N) to process NNPI or to connect to other IT systems that process NNPI.

c. The transportation of IT systems that process NNPI or NNPI IT media to locations outside the United States or its territories requires CNO (N00N) approval. The transport section in chapters 11, 12, and 13 provides additional details for obtaining CNO (N00N) approval for the respective type of IT addressed in the chapter.

d. Personally owned IT systems (such as a computer or mobile device) and IT media are prohibited from processing NNPI. The one exception for limited use of personally owned telecommunication systems for U-NNPI is addressed in chapter 12 of this instruction.

e. IT systems not accredited for NNPI that are involved in an authorized disclosure of NNPI are subject to response actions directed by the cognizant DAA with CNO (N00N) concurrence.

4. Audit and Review. All NNPI-authorized IT systems and all documentation associated therewith; NNPI IT media; and IT systems involved in the unauthorized disclosure of NNPI are subject to audit and review by CNO (N00N).

5. Deviations. Deviations from the requirements for control and protection of NNPI on IT systems prescribed in this instruction must be submitted in writing to CNO (N00N) for approval.

6. Contact. Questions concerning the control and protection of NNPI on IT systems or media required by this instruction should be addressed to the CNO (N00N) Director of Cybersecurity (DCS) at:

a. Director of Cybersecurity, SEA 08B
Naval Nuclear Propulsion Directorate
1240 Isaac Hull Avenue SE
Washington Navy Yard DC 20376-8011

b. 202-781-5931 for non-secure/commercial telephone communications;

c. <nnpi_dcs.fct@navy.mil> for unclassified email communications on Internet/non-classified Internet protocol router network (NIPRNET) (Note: this address may be listed as "NNPI_DCS" in exchange directories); or

d. <NNPI_DCS.fct@navy.smil.mil> for up to SECRET email communications on SIPRNET (Note: this address may be listed as "NNPI_DCS" in exchange directories).

# CHAPTER 10
# INFORMATION TECHNOLOGY (IT) RESPONSIBILITIES

1. General. This chapter assigns responsibilities for implementing and sustaining the control and protection of NNPI on Navy IT systems.

2. Information Owner. CNO (N00N) has statutory authority for the control and protection NNPI. Oversight of NNPI on IT has been delegated to the CNO (N00N) DCS.

a. The DCS is authorized to audit or review all IT systems that process (or are planned to process) NNPI. The DCS may designate agents to perform audits/reviews of NNPI on IT. DCS audits/reviews of NNPI on IT may include NNPP activities, Navy network operation centers, facilities, or support locations.

b. Under CNO (N00N)'s statutory authority, the DCS shall oversee cases of improper handling of NNPI and support the DAA investigations involving NNPI.

c. The DCS shall provide the DAA a determination of the suitability of an IT system to process NNPI as part of the certification and accreditation (C&A) process. DCS must concur before IT systems may be authorized to process NNPI.

3. DAA. The DAA formally assumes the responsibility for operating an IT system at an acceptable level of risk.

a. Reference (h) assigns Naval Network Warfare Command (NAVNETWARCOM) as the operational designated accrediting authority (ODAA) for any unclassified or classified IT systems owned or operated by, for, or on behalf of the Navy. Special cases in which another organization functions as the DAA are discussed below:

(1) Reference (h) authorizes the CO of a Navy vessel operating at sea to serve as a deployed DAA.

(2) Echelon 2 headquarters organizations may function as the DAA for research, development, test, and evaluation (RDT&E) networks as prescribed in reference (h).

(3) CNO (N00N) is the DAA for classified and unclassified information systems owned or operated by, for, or on behalf of CNO (N00N) and its Department of Energy (DOE) prime contractors.

(4) Defense Security Service is the DAA for classified information systems owned or operated by, for, or on behalf of the vendors supporting the Navy.

b. DAAs with overlapping responsibilities shall resolve any conflicts by formal written agreement.

c. NAVNETWARCOM and echelon 2 RDT&E DAAs shall:

(1) Accredit IT systems for NNPI per CNO (N00N) assessment:

(a) Incorporate CNO (N00N) review and concurrence into the C&A of systems that process (or are planned to process) NNPI.

(b) Obtain CNO (N00N) concurrence for NNPI processing before issuing an authorization (e.g., authorization to operate) for an IT system to process NNPI.

(2) Address unauthorized disclosures of NNPI:

(a) Inform CNO (N00N) of any potential, alleged, or actual compromise of NNPI on IT systems

(b) Develop and maintain systems and processes to report, respond, track, and resolve unauthorized disclosures or improper handling of NNPI on IT systems.

(c) Work to minimize the unauthorized disclosures of NNPI and to mitigate their impacts.

(d) Assist in investigating the improper handling of NNPI on IT systems by providing technical experts.

(e) Coordinate the mitigation and remediation strategy for any compromise of NNPI on IT systems not authorized to process NNPI.

(3) Include CNO (N00N) in IT infrastructure strategy and planning involving NNPI systems and support audits and reviews:

(a) Provide (or coordinate) access to personnel and training material associated with NNPI at the IT system operation centers, facilities, or support locations.

(b) Submit for CNO (N00N) concurrence any changes to policy or infrastructure (hardware or software) that may affect the security of NNPI before these changes are implemented.

(4) Serve as the primary point of contact on information assurance (IA) issues with IT systems processing NNPI.

(5) Consult CNO (N00N) on requirements for NNPI, such as:

(a) Providing CNO (N00N) a copy of all inquiries regarding NNPI protections and a copy of the proposed response for concurrence before issuing the response.

(b) Consulting with CNO (N00N) on clarifications to Navy requirements for the protection of NNPI.

4. Certification Authority (CA). Reference (h) assigns Space and Naval Warfare Systems Command (SPAWARSYSCOM) the responsibility as official Navy CA, which includes the comprehensive evaluation of the security features of an IT system and determining how well it meets security requirements. SPAWARSYSCOM shall submit completed risk assessments, including review of NNPI security controls, for systems involving NNPI to NAVNETWARCOM and CNO (N00N) during the certification process.

5. Program Manager. Reference (i) specifies that the program manager has overall business and funding responsibility for the IT system or application. In relation to NNPI, the program manager shall:

a. Adhere to requirements for safeguarding NNPI.

b. Incorporate NNPI protections into baseline requirements for IT systems that process or are planned to process NNPI.

c. Include CNO (N00N) in discussions or reviews required to clarify the proper safeguarding of NNPI on IT systems.

d. Include CNO (N00N) in discussions or reviews on IT systems and the IT services or capabilities NNPP needs.

e. Coordinate with the cognizant DAA, CNO (N00N), and CA personnel to properly test and evaluate systems and services involving NNPI.

f. Ensure that NNPI systems and services are properly included in overall lifecycle management planning for enterprise systems and services, such as sustainment, technology upgrades, and quality assurance.

g. Develop work processes to track and maintain formal communication with CNO (N00N) on IT systems containing NNPI.

6. Commanding Officer/Officer in Charge (CO/OIC). Per reference (i), the CO/OIC shall:

a. Serve as the local IA authority, including NNPI. CO/OICs are directly responsible for identifying vulnerabilities in their operational environments and for implementing the appropriate countermeasures.

b. Ensure that personnel under their command are trained in and abide by IA policy, including NNPI control and protection requirements.

c. Ensure that all IT assets they oversee and operate are accredited and operated in keeping with the C&A documentation.

d. Designate an NNPICO (per chapter 2 of this instruction) for activities processing NNPI on IT systems.

e. Appoint agents, as necessary, to review records associated with NNPI matters at the Navy network operation centers, facilities, or support locations.

7. Information Assurance Manager (IAM). Per reference (i), the IAM is responsible for IA within a command, site, or system.

a. The IAM is responsible to the local IA command authority and DAA for ensuring the security (including NNPI) of an IT system, and that it is approved, operated, and maintained throughout its lifecycle under the IT system's security C&A documentation. The IAM functions as the command's focal point for IA matters on behalf of, and principal advisor to, the DAA.

b. The IAM for a system shall develop C&A documents that include NNPI security controls per this instruction for IT systems that process (or are planned to process) NNPI.

c. IAMs will inform CO/OICs, NAVNETWARCOM, and CNO (N00N) of all NNPI incidents on Navy IT systems involving their command. For example:

(1) All inquiries regarding NNPI issues.

(2) Actual, potential, or alleged mishandling of NNPI.

(3) Navy IT system vulnerabilities involving risk of unauthorized access to NNPI.

8. Security Officer. Responsible for the physical protections for an activity, the security officer shall ensure the proper certification of NNPI workspaces, as well as validate U.S. citizenship and Government security clearances required for access to systems that process NNPI.

9. Users. Reference (i) specifies that users are individuals authorized to access an IT system. Authorized users of NNPI IT systems are responsible for protecting the NNPI they handle or process.

# CHAPTER 11
# INFORMATION SYSTEMS

1. General

a. This chapter specifies the security requirements for NNPI for Navy information systems that are certified and accredited by the Navy DAA or are designated as PIT by the DAA.

b. The NNPI requirements for C&A promote the secure operation of information systems. They establish minimum security levels and allow a more consistent, comparable, and repeatable approach for specifying security controls for information systems that process (or are planned to process) NNPI.

c. Reference (j) provides the Navy's IA policy and guidance for PIT. The Navy DAA may designate a PIT DAA per reference (j).

d. C&A of Navy information systems not designated as PIT follow the DoD Information Assurance Certification and Accreditation Process (DIACAP) in reference (k), as implemented by references (l) and (m). DIACAP covers the five cradle-to-grave stages of an information system, beginning with strategy and planning for IA and ending with the decommissioning of the information system. The IA program for the Navy is implemented by reference (h). The C&A for Navy information systems are tracked in the Information Assurance Tracking System (IATS) (or its planned replacement, the Certification and Accreditation Support Tool [CAST]). Information systems that adequately fulfill IA requirements (as determined by the CA) and that the DAA concurs in are granted authority to operate (ATO). The IAM and project manager (PM) or system manager (SM) serve key IA roles throughout the lifecycle of an information system.

e. CNO (N00N) DCS oversees NNPI security controls for PIT or information systems that process (or are planned to process) NNPI.

2. PIT. For systems designated as PIT under reference (j), the DAA or PIT DAA shall issue an ATO or interim ATO for PIT being authorized to process NNPI only with the concurrence of CNO (N00N).

3. Information Systems. Per reference (h), information systems not designated as PIT shall be certified and accredited by the Navy DAA.

a. For information systems planned to process NNPI that are now in DIACAP phase 1 (Initiate and Plan IA C&A), or that are initiated after the date of this instruction:

(1) In DIACAP phase 1 (Initiate and Plan IA C&A), the PM/SM shall include this instruction as a requirement and specifically incorporate table 3 into system security requirements, and include NNPI control in the strategy for protecting the system through its life.

(2) In DIACAP phase 2 (Implement and Validate Assigned IA Controls), the PM/SM shall evaluate tradeoffs between functional and NNPI security requirements, and document the decisions on the controls selected to meet the table 3 requirements. Security controls from reference (n) or reference (q) provide options to satisfy the table 3 requirements.

(a) A completed OPNAV 9210/1 shall be included in the executive DIACAP package in IATS (or CAST) for the information systems involving NNPI. This form is based on table 3 requirements. CNO (N00N) and NAVNETWARCOM may provide another template for use by NNPP activities in the C&A process.

(b) A separate detailed document that addresses the NNPI security controls implemented for the information system shall be included in the comprehensive DIACAP package in IATS (or CAST) for each information system involving NNPI. This detailed document substantiates compliance with the requirements in OPNAV 9210/1. This detailed document shall include:

1. The applicable requirements in OPNAV 9210/1.

2. The selected control(s), from either reference (n) or reference (q), for each requirement.

3. A description of its implementation for the information system.

Note: In each case where an OPNAV 9210/1 requirement is not met (indicated by no marking

of the box to “check if complies”), this detailed document must address how the risk of unauthorized disclosure of NNPI is reduced to an acceptable level without a security control to meet the requirement.

(3) In DIACAP phase 3 (Make Certification Determination and Accreditation Decision):

(a) The PM/SM shall validate that NNPI security requirements are met within the anticipated operational environment. Security accreditation must be completed before operational deployment of the system.

(b) The CA shall include an evaluation of NNPI during the certification review. The CA shall use OPNAV 9210/1 and supporting detailed documentation on NNPI security controls implemented for an information system submitted by the IAM/PM to conduct its independent verification and validation of the proper implementation of security controls for NNPI, assessment of compliance with security requirements for NNPI, determination of risk level for NNPI, and recommendation for accreditation to NAVNETWARCOM and CNO (N00N).

(c) The DAA shall issue an accreditation decision for information systems only with the concurrence of CNO (N00N) if that information system is being authorized to process NNPI.

(4) In DIACAP phase 4 (Maintain ATO and Conduct Reviews), the IAM shall:

(a) Control and monitor the operation of the information system to maintain (or restore in the case of incidents) an acceptable level of safeguarding for NNPI.

(b) Certify an annual review of an information system to (1) confirm the effectiveness of assigned IA controls (including NNPI) and their implementation or (2) recommend changes to the information system, develop plans to implement those changes, and obtain necessary recertification and reaccreditation of the information system.

(c) Recertify and reaccredit the information system (including the NNPI security controls) at least every 3 years

per reference (h). The DAA shall issue a reaccreditation for information systems involving NNPI only with CNO (N00N) concurrence.

(d) Ensure disposal or disposition of components of the information system determined to contain or possibly contain NNPI per chapter 6 this instruction.

(5) In DIACAP phase 5 (Decommissioning), the IAM shall:

(a) Ensure that any significant NNPI security control inheritance relationships are resolved before decommissioning the information system.

(b) Remove OPNAV 9210/1 and supporting detailed documentation on NNPI security control implementation for the information system from all tracking systems.

(c) Ensure disposal or disposition of components of the information system determined to contain or potentially contain NNPI per chapter 6 this instruction.

b. For information systems processing NNPI or planned to process NNPI that are in DIACAP phases 2 through 4 as of the date of this instruction:

(1) The IAM shall incorporate this instruction, including table 3, into the information system security requirements as discussed in subparagraph 3a(1) of this chapter.

(2) The IAM shall work with the PM to implement necessary changes to the information system to meet the revised NNPI requirements in this instruction.

(3) The associated NNPI documentation shall be updated during the course of the next C&A of the information system. The actions prescribed in subparagraph 3a(2) of this chapter shall be followed. Note: the implementation of security controls to meet the revised NNPI requirements and updates to the NNPI-related C&A items shall be accomplished by 3 years after the date of this instruction.

(4) After implementing changes to the information system to meet the revised NNPI requirements in this instruction, the actions prescribed in subparagraphs 3a(3) through 3a(5) of this chapter shall be followed.

c. Information systems that were being decommissioned before the date of this instruction shall dispose of information systems containing NNPI under pre-existing policies, guidelines, and standards. Information systems decommissioned on or after the date of this instruction shall follow the actions in subparagraph 3a(5) of this chapter.

4. User Authorization. Requirements for a user to be granted access to NNPI on a Navy information system that is approved for NNPI are as follows:

a. Validation by the security officer that the user (1) is a U.S. citizen, (2) is not operating for or on behalf of a foreign interest, and (3) for classified systems has the appropriate clearance for access to the information.

b. Signature of a supervisor attesting to the user's NTK for NNPI in the performance of assigned duties and responsibilities.

c. Acceptance by the user of IA responsibilities for NNPI on the Navy information system.

5. Transport. Transporting NNPI-related information systems outside the United States or its territories requires CNO (N00N) approval.

a. For information systems involving NNPI, NNPP activities must submit a security plan to CNO (N00N) for approval before transporting such items outside the United States or its territories. This security plan should address control of the equipment and the information it contains per this instruction, and should also address controls applied to the equipment from originating NNPP activity within the United States or its territories to the planned destination(s).

b. Information systems that have been procured for NNPI processing, but that have not yet been used for NNPI processing,

do not require special NNPI-related controls for transportation to locations outside the United States or its territories.

6. Deviations. Deviations from the requirements for control and protection of NNPI on information systems prescribed in this chapter must be submitted in writing to CNO (N00N) for approval.

# CHAPTER 12
# TELECOMMUNICATION SYSTEMS

1. General. This chapter specifies the requirements for processing NNPI on telecommunication systems. In relation to NNPI controls, telecommunications involve voice, fax, or video communications equipment that may be networked but are distinct from information systems that undergo a C&A process with a DAA. Voice, fax, or video equipment intended for NNPI use that is integrated into such information systems shall be addressed in the C&A of the host system or subsystem per the requirements in chapter 11.

2. Telecommunication Systems

a. NNPP activities shall manage telecommunication services, infrastructure, equipment, and personnel so as to prevent disclosure of NNPI to foreign nationals, the public, or others without an NTK. OPNAV 9210/1 provides requirements and comprehensive guidelines for NNPI control and protection items to be addressed. The NNPI control categories addressed and controls selected shall be tailored as appropriate for telecommunication systems covered in this chapter. Tailoring telecommunication controls to achieve adequate security for NNPI is a multifaceted, risk-based activity involving management and operational personnel within the organization.

b. For NNPI-related communications, regardless of location, individuals must be aware of their environment and take actions to avoid disclosure of NNPI to foreign nationals, the public, or others without an NTK.

c. Unless specifically addressed in this instruction, telecommunication systems or equipment without user-addressable electronic storage capabilities or with only volatile memory do not require marking or labeling for NNPI.

d. Classified NNPI telecommunications (including voice, video telephone conference (VTC), or fax) must use equipment and circuits authorized for classified processing in spaces designated for classified work. The circuits involved must encrypt transmissions by a method that meets NSA type-1 requirements (preferred method) or satisfies the requirements of reference (r). Classified NNPI telecommunication shall be only

at the level of information appropriate for the workspace by those individuals with an appropriate clearance and an NTK for NNPI.

e. U-NNPI-related telecommunications in areas outside the United States or its territories shall:

(1) Use Federal Information Protection Standard (FIPS) 140-2 certified or NSA type-1 encryption for all transmissions between end-points.

(2) Take place over devices issued, owned, or leased by an NNPP activity.

(3) Be conducted over lines (or channels, such as cellular) owned or leased by an NNPP activity.

(4) Involve only U.S. citizens with an NTK for U-NNPI in spaces where controls are implemented/maintained to prevent unfettered access or audiovisual monitoring/recording by the public, foreign nationals, or others without NTK for U-NNPI.

f. U-NNPI-related telecommunications in areas within the United States or its territories shall:

(1) For U-NNPI voice and fax:

(a) Take place over devices issued, owned, or leased by an NNPP activity.

(b) Be conducted over lines (or channels, such as cellular) owned or leased by an NNPP activity.

(c) Involve only U.S. citizens with an NTK for U-NNPI in spaces where controls are implemented/maintained to prevent unfettered access or audiovisual monitoring/recording by the public, foreign nationals, or others without NTK for U-NNPI.

(2) For U-NNPI VTC, follow the requirements provided in subparagraph 2e of this chapter.

(3) To the extent necessary to support NNPP operational needs, U-NNPI telecommunications within the United States or its territories in which the above subparagraphs 2f(1a) and 2f(1b)

requirements cannot be met, personally owned telecommunication devices (such as telephones, mobile phones, and fax machines) may be used provided the device is operated under the following restrictions:

(a) The device is not connected (wired, wireless, or other) to a computer (desktop, laptop, mobile, or other).

(b) Voice, video, photography, or faxes are not saved to any non-volatile storage within, attached, or connected to the device.

(c) Temporary storage is not retransmitted.

(d) The device does not use image-retaining print mechanisms (such as carbon or ink ribbon).

(e) Transcribing/conversion features or capabilities (such as voice to text) are not in operation.

(f) For faxes, the fax recipient must be present at the fax machine when the U-NNPI is transmitted by the sender; and the sender must confirm that the document was received by the recipient in its entirety.

3. Transport. Transporting NNPI-related telecommunication systems to locations outside the United States or its territories requires CNO (N00N) approval.

a. For telecommunication systems or equipment involving NNPI that does not involve a C&A process, NNPP activities must submit a security plan to CNO (N00N) for approval before transporting such items outside the United States or its territories. This security plan should address control of the equipment and the information it contains per this instruction. The security plan should address controls applied to the equipment from the originating NNPP activity within the United States or its territories to the planned destination(s).

b. Telecommunication systems and equipment that have been procured but not placed into use for NNPI processing or have only volatile memory or storage capabilities do not require special NNPI-related controls for transportation to locations outside the United States or its territories. Telecommunication

equipment with volatile memory or storage must be purged of NNPI before transport outside the United States or its territories.

4. Deviations. Waivers for the any of the above requirements or telecommunication capabilities not otherwise addressed involving NNPI must be formally submitted to CNO (N00N) for approval.

# CHAPTER 13
# OTHER ELECTRONICS

1. General. This chapter specifies the requirements for processing NNPI on electronics that are not otherwise covered under information systems (chapter 11) or telecommunication systems (chapter 12).

2. Other Electronics

a. Generally, electronics that connect to an information system are addressed in the C&A plan for the information system. Chapter 11 provides the requirements for information systems that process or are planned to process NNPI. Similarly, electronics involving NNPI connected to telecommunication systems should follow the requirements of chapter 12.

b. Electronics that process or are planned to process NNPI not otherwise addressed in chapter 11 (Information systems) or chapter 12 (Telecommunication systems) shall have the control and protection of NNPI for such items addressed in a security plan issued by the appropriate IAM and submitted to CNO (N00N) for information. This security plan may be a section in an existing local policy, instruction, manual, or other documentation.

(1) OPNAV 9210/1 provides requirements and comprehensive guidelines for items to be addressed regarding control and protection for NNPI on electronics addressed by this chapter. The NNPI control categories addressed and controls selected shall be tailored as appropriate for security plans developed for electronics covered in this chapter. The process of tailoring security controls for electronics to achieve adequate security for NNPI is a multifaceted, risk-based activity involving management and operational personnel within the organization.

(2) Policies and procedures play an important role in the effectiveness of NNPI information security for electronics. The success of security measures employed to protect NNPI relies on proper planning, implementation, and sustainment. NNPP activities must develop and promulgate formal, documented policies and procedures governing the NNPI control protection.

3. Transport. Transporting NNPI-related electronics addressed by this chapter to locations outside the United States or its territories requires CNO (N00N) approval.

a. For NNPI-related electronics addressed by this chapter, NNPP activities must submit a security plan to CNO (N00N) for approval before transporting such electronics outside the United States or its territories. This security plan should address control of the equipment and the information it contains per this instruction. The security plan should address controls applied to the equipment from originating NNPP activity within the United States or its territories to the planned destination(s).

b. NNPI-related electronics addressed by this chapter that have been procured, but not placed into use for NNPI processing or have only volatile memory or storage capabilities, do not require special NNPI related controls for transportation to locations outside the United States or its territories. Electronics with volatile memory or storage must be purged of NNPI before transport of the item outside the United States or its territories.

4. Deviations. Waivers for any of the above requirements involving NNPI must be formally submitted to CNO (N00N) for approval.

# APPENDIX A
# REFERENCES

(a) CG-RN-1, Rev. 3, DOE-DoD Classification Guide for the Naval Nuclear Propulsion Program (NOTAL)
(b) SECNAV M-5510.36 of 30 Jun 2006, Department of the Navy (DON) Information Security Program (ISP)
(c) NAVSEAINST 5230.12, Release of Information to the Public of 21 Nov 03
(d) NAVSEAINST 5510.2B, Physical Security, Access, and Movement Control at Shore Activities (NOTAL)
(e) DON Foreign Disclosure Manual of Sep 2007
(f) NAVSEA S9213-45-MAN-000(N) of Jul 2003, Naval Nuclear Material Management Manual (NOTAL)
(g) NIST Special Publication 800-88 of Sep 2006, Guidelines for Media Sanitization
(h) OPNAVINST 5239.1C
(i) SECNAV M-5239.1 of Nov 2005, DON IA Program
(j) DON CIO memo 02-10, IA Policy Update for PIT
(k) DoD Instruction 8510.01 of 28 Nov 2007
(l) DON CIO msg DTG 311917Z Mar 2008, DON's Transition Plan from DITSCAP to DIACAP
(m) DON DIACAP Handbook version 1.0 of 15 Jul 2008
(n) DoD Instruction 8500.2 of 6 Feb 2003
(o) DoD Policy Memorandum of 3 Jul 2007, Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media
(p) DoD Directive 8100.2 of 14 Apr 2004
(q) NIST Special Publication 800-53 of Aug 2009, Recommended Security Controls for Federal Information Systems
(r) NSTISSI No. 7003 of 13 Dec 96, Protective Distribution Systems (PDS)

## Useful Internet/NIPRNET Links for References

| Reference Type | Link |
|---|---|
| Committee on National Security Systems Issuances | <http://www.cnss.gov/issuances.html> |
| DoD Issuances | <http://www.dtic.mil/whs/directives/index.html> |
| DON Issuances | <http://doni.daps.dla.mil/default.aspx> |
| DON-CIO Policy & Guidance | <http://www.doncio.navy.mil/Policy.aspx> |
| NAVSEASYSCOM Issuances | <http://www.navsea.navy.mil/Organization/NAVSEA%20Instructions.aspx> |
| NIST Computer Security Resource Center – SP | <http://csrc.nist.gov/publications/PubsSPs.html> |

# APPENDIX B
# NAVAL NUCLEAR PROPULSION INFORMATION OVERVIEW

1. General. This appendix is provided as a training guide that can be removed from the body of this instruction and given to personnel/organizations to provide a better understanding of NNPI.

2. Definition. NNPI is defined as:

> Classified or unclassified information concerning the design, arrangement, development, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated nuclear support facilities.

3. Classified NNPI. Classified NNPI consists of two types of information--RD and national security information (NSI). Authority to classify NNPI comes from two sources: (1) the Atomic Energy Act of 1954 (as amended), which governs RD; and (2) Presidential Executive Order (EO) 13526 of December 2009 (as amended), which governs NSI. RD and NSI involving NNPI are usually at the CONFIDENTIAL level. However, there are instances of SECRET restricted data (SRD) and SECRET national security information (SNSI) involving NNPI. Further discussion of SECRET NNPI is provided in reference (a).

a. RD. The Atomic Energy Act covers information related to the use of special nuclear material. In the NNPP, this is information associated with the use of special nuclear material for the production of energy in the nuclear core. Per the Atomic Energy Act, access to RD requires an investigation on the character, associations, and loyalty of the individual concerned, as well as the subsequent granting of a final Government security clearance.

b. NSI. As defined in EO 13526, NSI is classified information in the following categories, which if disclosed, could be expected to cause damage to national security: military plans, weapons systems, or operations; foreign government information; intelligence activities, sources, or methods; foreign relations or foreign activities of the United States; scientific, technological, or economic matters relating

to national security; U.S. Government plans for safeguarding nuclear material or facilities; or vulnerabilities relating or capabilities of systems or installations relating to national security.

(1) E.O. 13526 prescribes a uniform system for classifying, declassifying, and safeguarding NSI.

(2) NNPI that is classified NSI must be protected from disclosure to foreign nationals. Consequently, classified NNPI that is NSI is also marked and handled as NOFORN to require access only by cleared U.S. citizens with an NTK unless specifically authorized by CNO (N00N).

(3) Personnel with an interim or final Government security clearance may access classified NNPI that is NSI.

4. U-NNPI. U-NNPI is controlled and protected under one or more of the following: (1) the Atomic Energy Act of 1954 (as amended), (2) the 1984 Defense Authorization Act, (3) Export Control Act Regulations of the Commerce Department, (4) Arms Export Control Act Regulations (i.e., International Traffic in Arms Regulations (ITAR); Munitions List), (5) Export of Sensitive Nuclear Information for Foreign Atomic Energy Regulations of the Energy Department.

a. U-NNPI is information related to sensitive military technology (i.e., naval nuclear propulsion technology).

b. Access to U-NNPI is limited to U.S. citizens with an NTK.

c. No clearance is required for access to U-NNPI.

d. U-NNPI is marked and handled as NOFORN.

# APPENDIX C
# SAMPLE SECURITY AGREEMENT FOR PROTECTION OF U-NNPI

1. Purpose. The undersigned hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to Federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by anyone not having a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

2. Specific Requirements for Protecting U-NNPI

a. Only U.S. citizens who have an NTK required to execute the contract shall be allowed access to U-NNPI.

b. When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe). Access to the container must be such that only authorized persons can access it, and compromise of the container would be obvious at sight. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured (e.g., in a home or automobile, or unattended in a motel room or sent with baggage).

c. U-NNPI documents will have the word NOFORN at the top and bottom of each page. The cover sheet will have the warning statement shown below. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such as video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.

**NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command.

**Note: This distribution warning statement is for training purposes only.**

d. U-NNPI may not be processed on networked computers with outside access unless approved by CNO (N00N). If desired, the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, such as personal computers, laptops, personal digital assistants, and other portable electronic devices are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and CNO (N00N).

e. U-NNPI may be faxed within the continental United States and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental United States, including military installations, unless encrypted by means approved by CNO (N00N).

f. U-NNPI may be sent within the continental United States and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.

g. Documents containing U-NNPI shall be disposed of as classified material.

h. Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.

i. Report any compromises of U-NNPI to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on Web site, transmission via email, or violation of the information system containing U-NNPI.



_____ _____

Signature Date

# APPENDIX D
# ACRONYMS AND DEFINITIONS

1. Acronyms

| | |
|---|---|
| ATO | authority to operate |
| C&A | certification and accreditation |
| CA | certification authority |
| CAST | Certification and Accreditation Support Tool |
| CD | compact disk |
| CNO | Chief of Naval Operations |
| CNSI | CONFIDENTIAL national security information |
| CNO (N00N) | Director, Naval Nuclear Propulsion Program |
| CO | commanding officer |
| CO/OIC | commanding officer/officer in charge |
| CRD | CONFIDENTIAL restricted data |
| DAA | designated accrediting authority |
| DCS | Director of Cybersecurity |
| DIACAP | DoD Information Assurance Certification and Accreditation Process |
| DoD | Department of Defense |
| DOE | Department of Energy |
| DOE-UCNI | Department of Energy – Unclassified Controlled Nuclear Information |
| DON | Department of Navy |
| DVD | digital video disk |
| EO | executive order |
| FIPS | Federal Information Protection Standard |
| IA | information assurance |
| IAM | information assurance manager |
| IATS | Information Assurance Tracking System |
| IT | information technology |
| ITAR | International Traffic in Arms Regulations |
| NAVICP | Naval Inventory Control Point |
| NAVSEASYSCOM | Naval Sea Systems Command |
| NIST | National Institute of Standards and Technology |
| NNPI | naval nuclear propulsion information |
| NNPICO | naval nuclear propulsion information control officer |
| NNPP | Naval Nuclear Propulsion Program |
| NAVNETWARCOM | Naval Network Warfare Command |
| NOFORN | not releasable to foreign nationals |
| NOTAL | not to all |
| NSA | National Security Agency |

| | |
|---|---|
| NSI | national security information |
| NTK | need-to-know |
| ODAA | operational designated accrediting authority |
| OSH | occupational safety and health |
| PIT | platform information technology |
| PM | project manager |
| PROM | programmable read-only memory |
| RD | restricted data |
| RDT&E | research, design, test, and evaluation |
| SECNAV | Secretary of the Navy |
| SM | system manager |
| SMIC | special material identification code |
| SNSI | SECRET national security information |
| SPAWARSYSCOM | Space and Naval Warfare Systems Command |
| SRD | SECRET restricted data |
| SUPSHIP | supervisor of shipbuilding |
| UCNI | UNCLASSIFIED controlled nuclear information |
| U-NNPI | UNCLASSIFIED naval nuclear propulsion information |
| USB | universal serial bus |
| VTC | video telephone conference |

2. Terms Defined. The following terms and definitions, listed in alphabetical order, are provided to aid in interpreting this instruction.

a. Accreditation. The formal declaration by the DAA that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

b. Certification. The comprehensive evaluation of the technical and non-technical security features of an information system and determining the degree to which the information system meets its specified security requirements.

c. DOE Unclassified Controlled Nuclear Information (DOE-UCNI). DOE-UCNI involves information protected under section 148 of the Atomic Energy Act. One part of DOE-UCNI includes information pertaining to the reactor plants of naval nuclear propulsion plants. Documents containing unclassified DOE reactor plant information may be marked with a DOE-UCNI warning statement when they are sent to Navy activities. The protection requirements are the same as those for U-NNPI. Therefore, documents marked as DOE- UCNI will be protected as U-NNPI.

(Note: DoD UCNI relates solely to information regarding protection of special nuclear material for weapons and does not include reactor plant information.)

d. Dual Citizens. Individuals who are dual citizens (hold both a U.S. citizenship and the citizenship of some other country). Such individuals are subject to special restrictions.

e. Foreign Interest. Any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or entity organized under the laws of any country other than the United States or its possessions; and any foreign national. Firms organized under U.S. laws, regardless of potential foreign ownership, can receive contracts requiring access to U-NNPI if the firm formally agrees to protect the information.

f. Foreign National. For the purposes of this instruction, a foreign national is any person not a U.S. citizen. Non-U.S. citizens permanently residing in the United States are considered foreign nationals.

g. Information System. A discrete set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

h. Information Technology (IT). Any equipment or inter-connected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

i. Naval Nuclear Propulsion Information (NNPI). All classified or unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.

j. Need-to-Know (NTK). An official determination that a proposed recipient's access to information is necessary in the performance of official or contractual duties of employment.

k. NNPI Control Officer (NNPICO). The individual who is both familiar with NNPI and its protection requirement and designated by an activity that routinely deals with NNPI. Each activity shall ensure that the NNPICO is technically qualified, or that a technically qualified person shall be available for consultation. The NNPICO's primary responsibility shall be to ensure that only site personnel with an NTK are granted and allowed to retain access to NNPI.

l. NNPI Workspace. An area designated by the Government where NNPI may be processed.

m. NNPP Activity. Organizations that have an officially assigned or contracted function that involves the research, design, construction, testing, operation, maintenance, or disposal of naval nuclear propulsion plants.

n. Representative of a Foreign Interest. For the purposes of this instruction, a representative of a foreign interest is any person, regardless of citizenship, functioning (in an individual capacity or on behalf of any corporation, person, or government entity) as an official, representative, agent, or employee of a foreign interest. One exception is that U.S. citizens appointed by their U.S. employer to act as a representative in the management of a foreign subsidiary of a U.S. corporation will not be considered representatives of a foreign interest.

o. Restricted Data (RD). A special type of classified information as defined in section 11(w) of Public Law 83-703 (The Atomic Energy Act of 1954, as amended), as ". . . all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142."

**TABLE 1**
**ACCESS REQUIREMENTS SUMMARY**

| Classification and Handling Controls | Governing Laws | Minimum Information Access Requirements |
|---|---|---|
| U-NNPI<br><br>Which is marked and handled as: NOFORN | • Atomic Energy Act of 1954, as amended<br>• Commerce Department Export Control Act<br>• Arms Export Control Act Regulations (ITAR/Munitions)<br>• DOE Regulations for Export of Sensitive Nuclear Information<br>• 1984 DoD Authorization Act Regulations | • U.S. citizenship<br>• NTK |
| CRD | • Atomic Energy Act of 1954, as amended | • U.S. citizenship<br>• NTK<br>• FINAL* CONFIDENTIAL Clearance |
| CNSI | • EO 13526 of December 2009, as amended | • U.S. citizenship<br>• NTK<br>• Interim CONFIDENTIAL Clearance |
| SRD | • Atomic Energy Act of 1954, as amended | • U.S. citizenship<br>• NTK<br>• FINAL** SECRET Clearance |
| SNSI | • EO 13526 of December 2009, as amended | • U.S. citizenship<br>• NTK<br>• Interim SECRET Clearance |

* **Note**: Even if an individual is granted a clearance for information of a higher classification than CONFIDENTIAL, the clearance must be adjudicated as FINAL before access to CRD may be granted.

** **Note**: Even if an individual is granted a clearance for information of a higher classification than SECRET, the clearance must be adjudicated as FINAL before access to SRD may be granted.

# TABLE 2
# SYSTEMS AND COMPONENTS
# (PLACEHOLDER)

1. General

a. This placeholder is incorporated into the unclassified portion of OPNAVINST N9210.3 that is used for unclassified-only access within the Navy, such as the unclassified-only Department of the Navy Issuances Web site <http://doni.daps.dla.mil>. Instructions on how to obtain table 2 are provided below.

b. Table 2 is U-NNPI/NOFORN because it is a compilation of reactor and propulsion plant systems and equipment that reveals information regarding the basic propulsion plant design of Navy nuclear-powered warships. Table 2 is available, upon request, for NNPP activities. Requests for table 2 should be made to:

Director of Security, SEA 08B
Naval Nuclear Propulsion Directorate
1240 Isaac Hull Avenue SE
Washington Navy Yard DC 20376-8011
(202) 781-6296

c. Additionally, the complete version of OPNAVINST N9210.3 that includes table 2 is available on the SIPRNET Department of the Navy Classified Issuances Web site at <http://hqweb.cno.navy.smil.mil/donci>.

# TABLE 3
# IT CONTROL REQUIREMENTS FOR NNPI

Also refer to OPNAV 9210/1 IT Checklist for NNPI, which is based on this table and can be obtained from Naval Forms Online at <http://navalforms.daps.dla.mil>.

**U-NNPI IT Systems:** Requirements in 1-18 apply.
**U-NNPI IT Media:** Requirements in 10 and 18.2-18.5 apply.
**Classified NNPI IT Systems:** Requirements in 1-17 and 19 apply.
**Classified NNPI IT Media:** Requirements in 10 and 19.2-19.5 apply.

| |
|---|
| **1. Access Control** |
| 1.1 Controls are implemented/maintained to limit NNPI access to authorized NNPI users, to processes acting on behalf of authorized users or devices (including other information systems), and to the types of transactions and functions authorized users are permitted to exercise. |
| 1.2 Controls are implemented/maintained to limit NNPI access with hardware and system configurations in such a manner that the IT users may not compromise them. |
| **2. Awareness and Training** |
| 2.1 Controls are implemented/maintained to ensure that managers and users of the information systems processing NNPI know about the security risks associated with their activities and the applicable laws, EOs, directives, policies, standards, instructions, regulations, or procedures related to the security of information systems and NNPI. |
| 2.2 Controls are implemented/maintained to ensure that personnel are adequately trained to carry out their assigned NNPI information security-related duties and responsibilities. |
| 2.3 Controls are implemented/maintained to ensure that all NNPI users receive initial and annual refresher NNPI training. Records of training for the most recent training received by users shall be retained. |
| 2.4 Controls are implemented/maintained to ensure that each NNPI users has a signed user agreement on record prior to being granted access to NNPI on the information system. |
| **3. Audit and Accountability** |
| 3.1 Controls are implemented/maintained to create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity involving NNPI. |
| 3.2 Controls are implemented/maintained to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. |
| **4. Certification, Accreditation, and Security Assessments** |
| 4.1 NNPI controls on the information system are periodically (at least annually) assessed to determine if the controls are effective. |

**TABLE 3 (CONT'D)**
**IT CONTROL REQUIREMENTS FOR NNPI**

| |
|---|
| 4.2 Controls are implemented/maintained to ensure that privileged users develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities to unauthorized disclosure or spillage of NNPI on the information system. |
| 4.3 Controls are implemented/maintained to ensure that only authorized information systems interconnection(s) are implemented. |
| 4.4 Information system security controls for NNPI are monitored on an ongoing basis to ensure the continued effectiveness of the controls. |
| **5. Configuration Management** |
| 5.1 NNPI controls are implemented/maintained on the information system to establish and maintain baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. |
| 5.2 NNPI controls are implemented/maintained on the information system to establish and enforce security configuration settings for information technology products employed in information systems. |
| **6. Contingency Planning** |
| 6.1 NNPI controls are incorporated into organizational efforts to establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources (including NNPI) and continuity of operations in emergency situations. |
| **7. Identification and Authentication** |
| 7.1 Controls are implemented/maintained to identify NNPI information system users, processes acting on behalf of NNPI users, or NNPI devices and authenticate (or verify) the identities of those authorized NNPI users, processes, or devices, as a prerequisite to allowing access to NNPI on information systems. |
| **8. Incident Response** |
| 8.1 Controls are implemented/maintained for an operational NNPI incident handling capability for information systems that include adequate preparation, detection, analysis, containment, recovery, and user response activities. |
| 8.2 Controls are implemented/maintained to track, document, and report NNPI incidents to appropriate organizational officials and or authorities (such as the DAA). |
| 8.3 Controls are implemented/maintained for verifying the occurrence of unauthorized or inadvertent disclosures of NNPI and reporting verified incidents to the ODAA and CNO (N00N). Suspected unauthorized or inadvertent disclosures of U-NNPI shall be verified and reported, if confirmed, within 24 hours. Unauthorized or inadvertent disclosures of classified NNPI shall be verified and reported, if confirmed, within 8 hours. |

**TABLE 3 (CONT'D)**
**IT CONTROL REQUIREMENTS FOR NNPI**

| |
|---|
| 8.4 Controls are implemented/maintained for responding to and resolving incidents of unauthorized or inadvertent disclosures of NNPI. U-NNPI incidents shall be resolved and closed within 30 calendar days of initial reporting. Classified NNPI incidents shall be resolved within 14 calendar days of initial reporting. |
| **9. Maintenance** |
| 9.1 Controls are implemented/maintained to perform periodic and timely maintenance on information systems involving NNPI. |
| 9.2 Controls are implemented/maintained for the tools, techniques, mechanisms, and personnel used to conduct information system maintenance to preclude foreign national or unauthorized access to NNPI. |
| **10. Media Protection** |
| 10.1 Controls are implemented/maintained to protect NNPI on information system equipment and IT media. |
| 10.2 Controls are implemented/maintained to limit access to NNPI on IT media to authorized NNPI users. |
| 10.3 Controls are implemented/maintained to dispose of NNPI IT media per chapter 6 of this instruction. |
| 10.4 Controls are implemented/maintained to ensure that NNPI IT media is disposed of when no longer needed or accumulated for disposal at a periodicity not longer than a calendar year. |
| 10.5 Controls are implemented/maintained to ensure that unattended IT media containing NNPI (classified or unclassified) has adequate physical protections commensurate with the level of information they contain. |
| 10.6 Controls are implemented/maintained for ingress and egress controls for NNPI IT media and equipment per this instruction and DAA policy. |
| 10.7 Controls are implemented/maintained to ensure that IT media used to transfer NNPI to or from information systems accredited for NNPI are used only for required business/work purposes and are not used to introduce malicious code, vulnerabilities, or mechanisms for the collection or redirection of information processed on the information system. |
| 10.8 Controls are implemented/maintained to ensure that IT media used for NNPI are only used on information systems with an accreditation for NNPI commensurate with the highest level and most restrictive controls required for the IT media. Reuse of IT media containing NNPI on a less restrictive or low classification of information system is prohibited. |
| **11. Physical and Environmental Protection** |
| 11.1 Controls are implemented/maintained to prevent physical access to information systems, equipment, IT media, and the respective operating environments involving NNPI by foreign nationals or others without an NTK per this instruction. |
| 11.2 Controls are implemented/maintained to protect the physical plant and support infrastructure for information systems processing NNPI. |

**TABLE 3 (CONT'D)**
**IT CONTROL REQUIREMENTS FOR NNPI**

| |
|---|
| 11.3 Controls are implemented/maintained to limit physical access to NNPI IT resources in manner that is commensurate with the classification and handling requirements for the information processed. These controls shall be in place to prevent unauthorized physical access, tampering, damage, and theft. This can be achieved by controlling access into specific areas or by controlling access to specific resources (e.g., personal computers, printers, servers, network devices, wiring closets, etc.). |
| **12. Planning** |
| 12.1 Controls are implemented/maintained to develop, document, periodically update, and implement security plans for information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing NNPI. |
| **13. Personnel Security** |
| 13.1 Controls are implemented/maintained to ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria (including NNPI) for those positions. |
| 13.2 Controls are implemented/maintained to ensure that NNPI and information systems are protected during and after personnel actions, such as terminations and transfers. |
| 13.3 Controls are implemented/maintained to employ formal sanctions for personnel failing to comply with organizational security policies and procedures regarding NNPI. |
| **14. Risk Assessment** |
| 14.1 Controls are implemented/maintained to periodically assess the risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of information systems and the associated processing, storage, or transmission of NNPI. |
| **15. System and Services Acquisition** |
| 15.1 Controls are implemented/maintained to allocate sufficient resources to adequately protect information systems with regards to NNPI processing needs. |
| 15.2 Controls are implemented/maintained to employ system development life cycle processes that incorporate NNPI information security considerations. |
| 15.3 Controls are implemented/maintained to employ necessary software usage and installation restrictions regarding NNPI processing. |
| 15.4 Controls are implemented/maintained to ensure that third-party providers employ adequate NNPI security measures to protect information, applications, and or services outsourced from the organization. |
| **16. System and Communications Protection** |
| 16.1 Controls are implemented/maintained to monitor, manage, and protect organizational communications (i.e., information transmitted or received by information systems) at the external boundaries and key internal boundaries of the information systems processing NNPI. |

**TABLE 3 (CONT'D)**
**IT CONTROL REQUIREMENTS FOR NNPI**

| |
|---|
| 16.2 Controls are implemented/maintained to employ architectural designs, software development techniques, and systems engineering principles that promote effective NNPI security within information systems. |
| **17. System and Information Integrity** |
| 17.1 Controls are implemented/maintained to identify, report, and correct information and information system flaws affecting NNPI related controls in a timely manner. |
| 17.2 Controls are implemented/maintained to provide protection from malicious code at appropriate locations within information system processing NNPI. |
| 17.3 Controls are implemented/maintained to monitor information system security alerts and advisories for NNPI and take appropriate actions in response. |
| **18. U-NNPI Specifications (U-NNPI Systems Only)** |
| 18.1 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for data in transit on information systems used to process up to U-NNPI. |
| 18.2 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for data at rest on mobile client devices processing up to U-NNPI. |
| 18.3 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is implemented for all removable IT media (including peripheral electronic storage) containing up to U-NNPI. IT media includes, but is not limited to, optical media (such CDs or DVDs), USB thumb drives, media cards, and external hard-drives. |
| 18.4 Controls are implemented/maintained to ensure that IT equipment, media, electronic displays, and other IT items for U-NNPI are marked or labeled per chapter 2 of this instruction. |
| 18.5 Controls are implemented/maintained to ensure that U-NNPI IT media and equipment are disposed of per chapter 6 of this instruction. |
| 18.6 Controls are implemented/maintained to ensure that users are prompted to accept the following terms during the initial logon for each session that includes access to U-NNPI:<br><br>*You are approved to process up to and including unclassified naval nuclear propulsion information (U-NNPI) on this system.*<br><br>*U-NNPI is not for release to foreign nationals (NOFORN) and has special handling requirements. U-NNPI is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of the Director, Naval Nuclear Propulsion Program (CNO (N00N)). It is your responsibility to protect U-NNPI from disclosure to individuals without a need-to-know.*<br><br>*You are not approved to process classified information on this system.* |

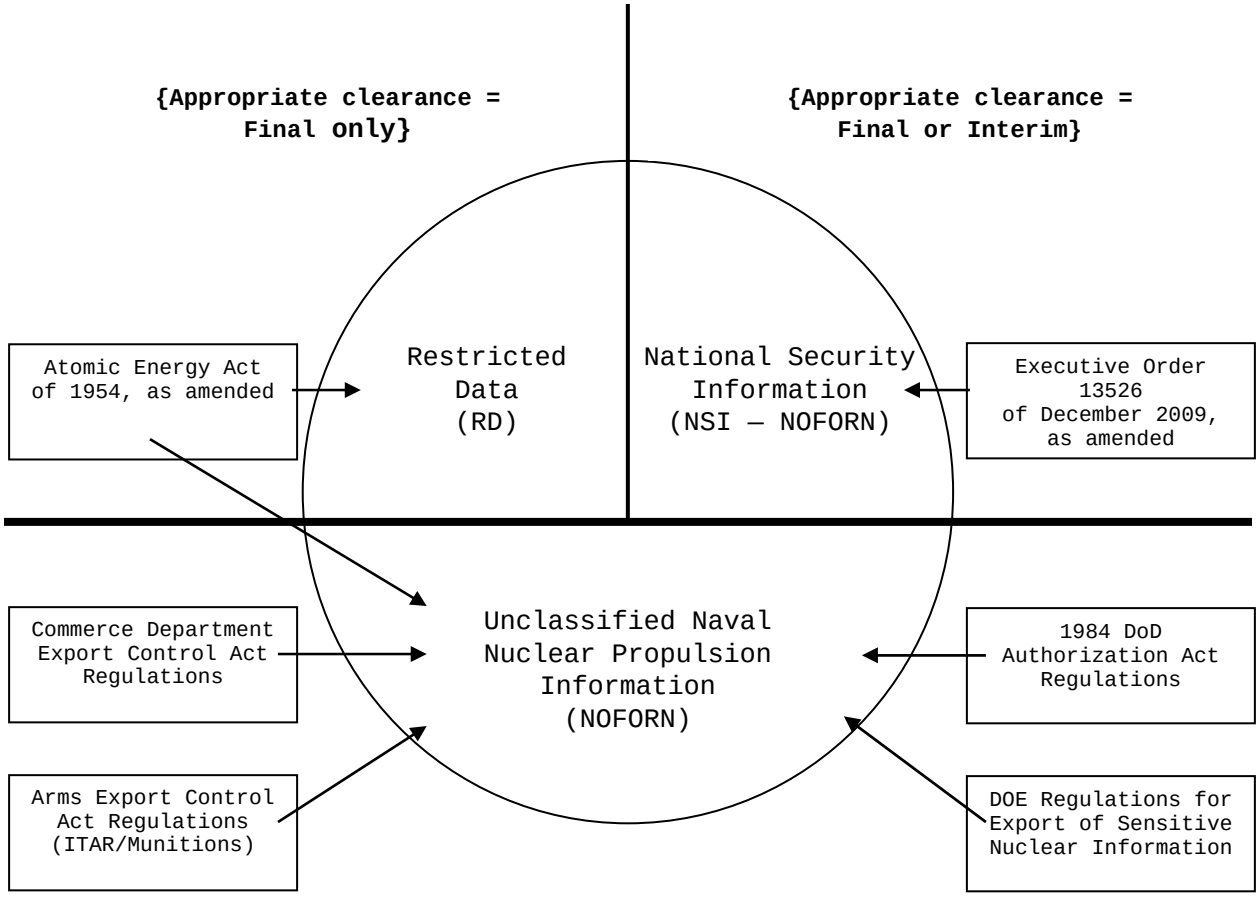
**TABLE 3 (CONT'D)**
**IT CONTROL REQUIREMENTS FOR NNPI**

| **19. Classified NNPI Specifications (Classified NNPI Systems Only)** |
|---|
| 19.1 Controls are implemented/maintained to ensure an NSA type-1 certified encryption is implemented for data in transit or protected distribution systems are used per the requirements of reference (r) on information systems used to process classified NNPI. |
| 19.2 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for data at rest on mobile client devices processing classified NNPI until an NSA type-1 certified encryption product for data at rest is available, at which time the NSA type-1 certified encryption product shall be used for data at rest on mobile client devices processing classified NNPI. |
| 19.3 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for all removable IT media (including peripheral electronic storage) containing classified NNPI until an NSA type-1 certified encryption product for data at rest is available, at which time the NSA type-1 certified encryption product shall be used for all removable IT media (including peripheral electronic storage) containing classified NNPI. IT media includes, but is not limited to, optical media (such CDs or DVDs), USB thumb drives, media cards, and external hard-drives. |
| 19.4 Controls are implemented/maintained to ensure that IT equipment, media, electronic displays, and other IT items for classified NNPI are marked or labeled per chapter 2 of this instruction. |
| 19.5 Controls are implemented/maintained to ensure that classified NNPI IT media and equipment are disposed of per chapter 6 of this instruction. |
| 19.6 Controls are implemented/maintained to ensure that a classified NNPI user on IT systems authorized up to the CONFIDENTIAL or SECRET level are prompted to accept the following terms during the initial logon for each session that includes access to classified NNPI:<br><br>*You are approved to process up to and including* [*CONFIDENTIAL* or *SECRET* as appropriate] *naval nuclear propulsion information (NNPI) on this system.*<br><br>*NNPI is not for release to foreign nationals (NOFORN) and has special handling requirements. NNPI is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of the Director, Naval Nuclear Propulsion Program (CNO (N00N)). It is your responsibility to protect NNPI from disclosure to individuals without a need-to-know.*<br><br>*Access to RESTRICTED DATA (RD) NNPI requires FINAL Government clearance. It is your responsibility to protect RD NNPI from disclosure to individuals without a final clearance.* |

# EXHIBIT 1
# ACCESS REQUIREMENTS SUMMARY

## CLASSIFIED NAVAL NUCLEAR PROPULSION INFORMATION (NNPI) —— SECRET OR CONFIDENTIAL

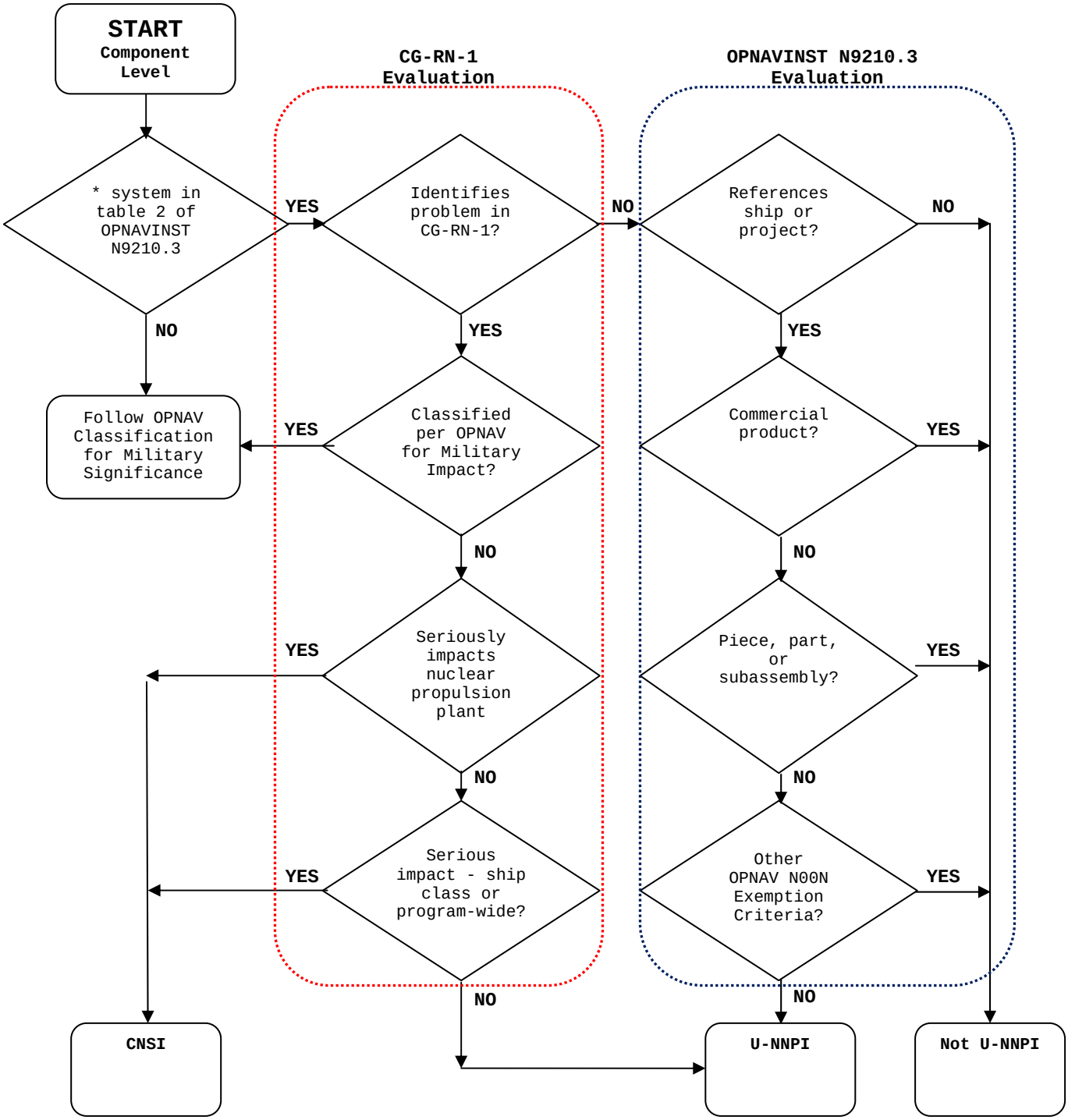
**{Overall access requirements = U.S. citizenship + appropriate clearance + need-to-know}**




## UNCLASSIFIED NAVAL NUCLEAR PROPULSION INFORMATION (U-NNPI)

{Overall access requirements = U.S. citizen + need-to-know}

# EXHIBIT 2
# COMPONENT LEVEL DETERMINATION FLOWCHART



# EXHIBIT 3
## MARKING REQUIREMENTS AND DISTRIBUTION WARNING STATEMENTS

1. Markings. The markings in this exhibit are required for the top and bottom of all pages of the associated NNPP document. The marking may be done by stamp or printed in a large font, bold, all capital letters, centered (left to right). The recommended font for most of the markings of this exhibit is Arial boldface 24 point. For the full-text markings on UCNI Arial boldface 16 point is recommended. Markings in color (as shown) are preferred, but not required.

2. Distribution Warning Statements. Note: "Distribution F" statements are not required for NNPI documents. The appropriate distribution warning statement(s) from this exhibit shall be placed on the cover page and or first page of all NNPI documents. The distribution warning statements should be placed in the lower left-hand corner above the classification or handling marking at the bottom of the page. When there are two statements, as in the case of CNSI, the second statement is usually placed on the lower right-hand corner above the classification or handling marking at the bottom of the page. The recommended font for distribution warning statements is Arial 8 point. The box surrounding the distribution warning statement, as done in this exhibit, is preferred, but not required.

3. DOE Unclassified Controlled Nuclear Information (DOE–UCNI) (Note: May be received by the shipyard from DOE.)

Marking requirement

**UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION**

**or**

**UCNI**

Distribution warning statement

**UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION:** Not for public dissemination. Unauthorized dissemination is subject to civil and criminal sanctions under Sec. 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168).

4. U–NNPI. See the exhibit 4 sample.

Marking requirement

**NOFORN**

Distribution warning statement

**NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command.

5. CRD. See the exhibit 5 sample.

Marking requirement

**CONFIDENTIAL**

or

**CONFIDENTIAL — RESTRICTED DATA**

Distribution warning statement

Derived from: DOE-DOD Classification Guide CG-RN-1
**RESTRICTED DATA**
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

6. CNSI. See the exhibit 6 sample.

Marking requirement

**CONFIDENTIAL**

or

**CONFIDENTIAL — NOFORN**

Distribution warning statements. There are two statements. The NSI statement is usually placed in the lower left-hand corner and the NOFORN statement is placed in the lower right-hand corner.

Classified by: _____
Derived from: DOE-DOD Classification Guide CG-RN-1
Declassify on: 25X4, 25X6; EV.
This document shall not be used as a basis for derivative classification guidance.

**NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command.

7. SRD

Marking requirement

**SECRET — RESTRICTED DATA**

Distribution warning statement

Derived from: DOE-DOD Classification Guide CG-RN-1
**RESTRICTED DATA**
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

8. SNSI

Marking requirement

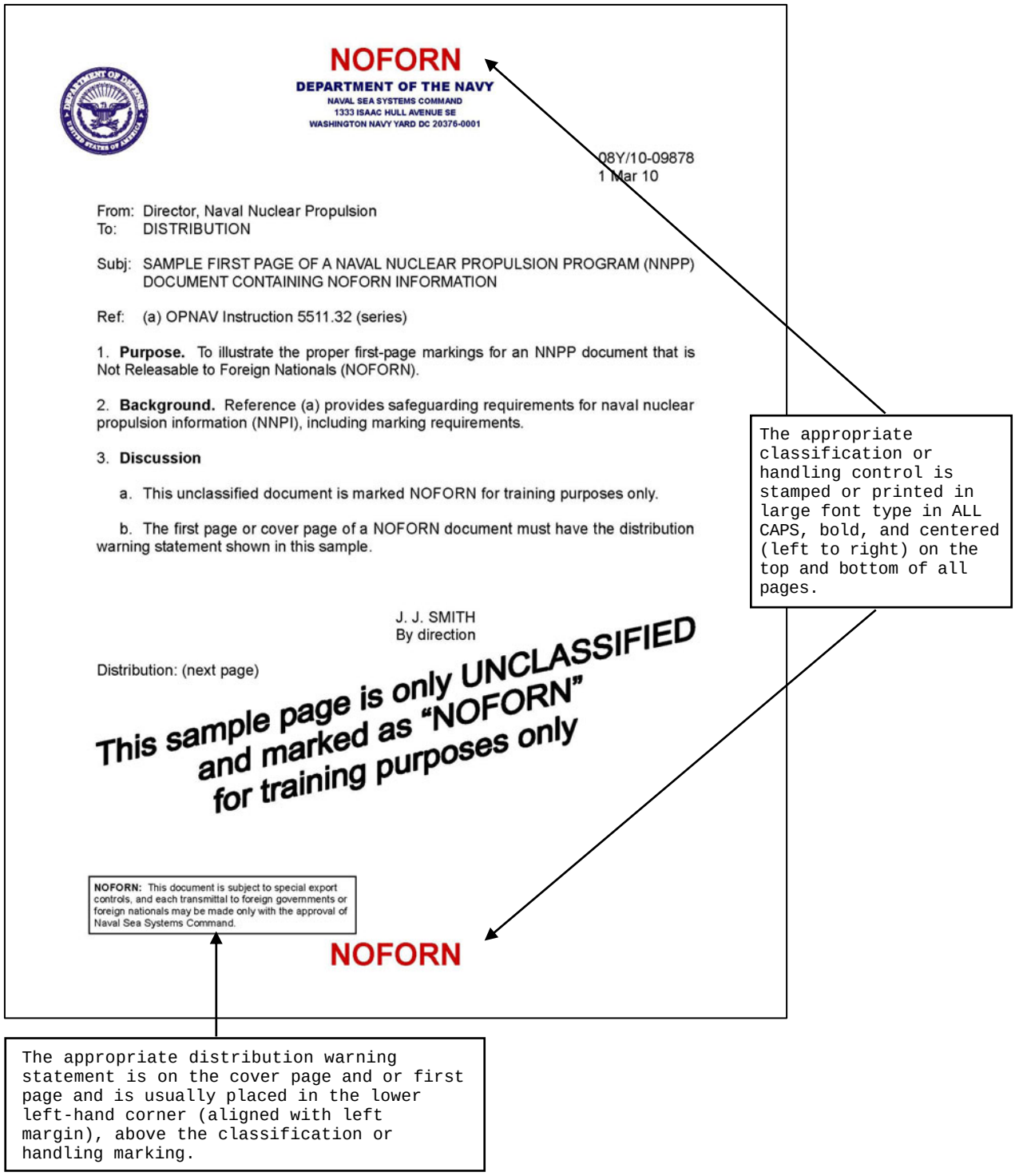
**SECRET — NOFORN**

Distribution warning statements. There are two statements. The NSI statement is usually placed in the lower left-hand corner and the NOFORN statement is placed in the lower right-hand corner.

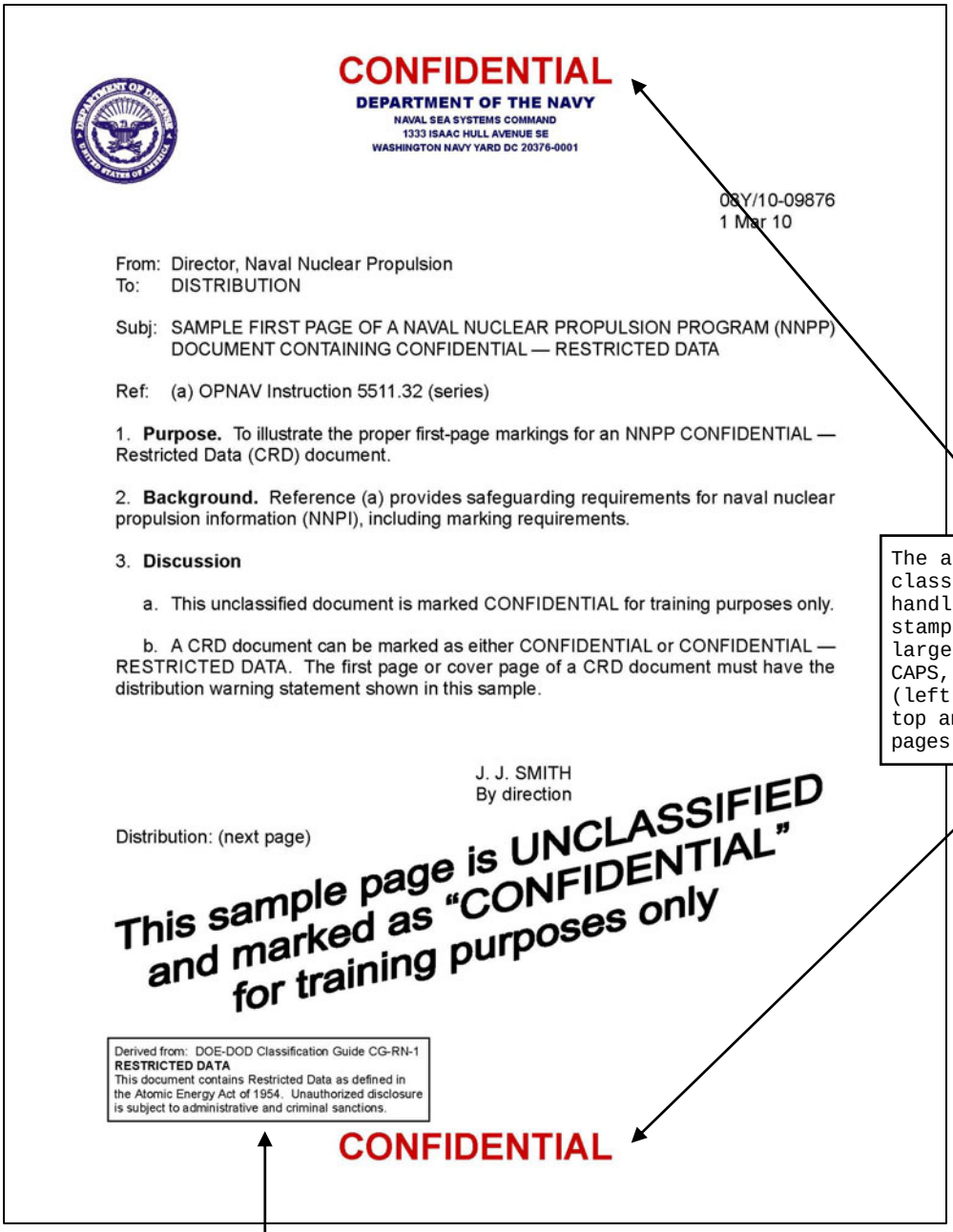
Classified by: _____
Derived from: DOE-DOD Classification Guide CG-RN-1
Declassify on: 25X4, 25X6; EV.
This document shall not be used as a basis for derivative classification guidance.

**NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command.

# EXHIBIT 4
# SAMPLE OF NOFORN MARKINGS



# EXHIBIT 5
# SAMPLE OF CRD MARKINGS



CONFIDENTIAL

DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
1333 ISAAC HULL AVENUE SE
WASHINGTON NAVY YARD DC 20376-0001

08Y/10-09876
1 Mar 10

From: Director, Naval Nuclear Propulsion
To: DISTRIBUTION

Subj: SAMPLE FIRST PAGE OF A NAVAL NUCLEAR PROPULSION PROGRAM (NNPP) DOCUMENT CONTAINING CONFIDENTIAL — RESTRICTED DATA

Ref: (a) OPNAV Instruction 5511.32 (series)

1. **Purpose.** To illustrate the proper first-page markings for an NNPP CONFIDENTIAL — Restricted Data (CRD) document.

2. **Background.** Reference (a) provides safeguarding requirements for naval nuclear propulsion information (NNPI), including marking requirements.

3. **Discussion**

a. This unclassified document is marked CONFIDENTIAL for training purposes only.

b. A CRD document can be marked as either CONFIDENTIAL or CONFIDENTIAL — RESTRICTED DATA. The first page or cover page of a CRD document must have the distribution warning statement shown in this sample.

J. J. SMITH
By direction

Distribution: (next page)

This sample page is UNCLASSIFIED and marked as "CONFIDENTIAL" for training purposes only

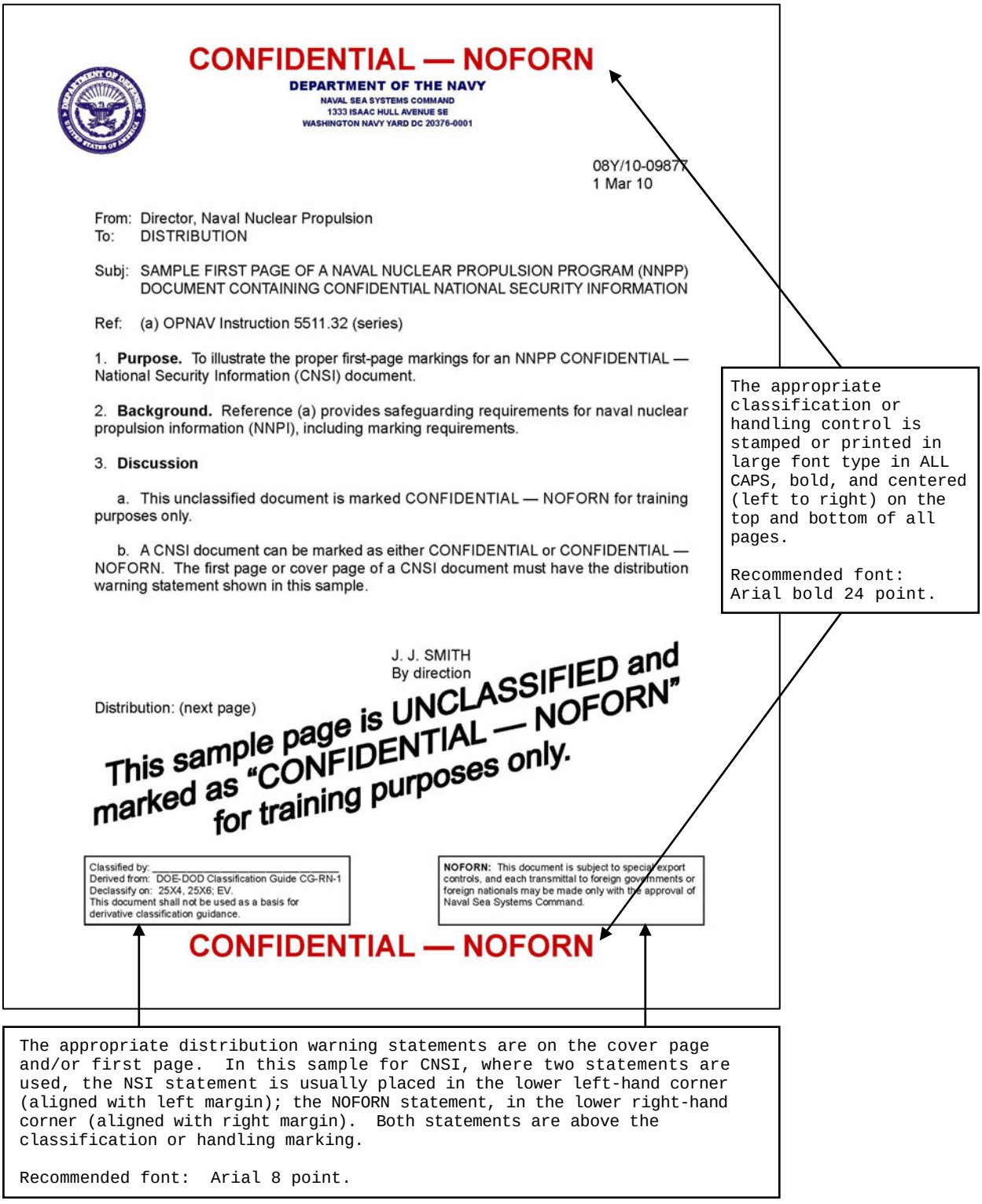
Derived from: DOE-DOD Classification Guide CG-RN-1
**RESTRICTED DATA**
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

CONFIDENTIAL

The appropriate classification or handling control is stamped or printed in large font type in ALL CAPS, bold, and centered (left to right) on the top and bottom of all pages.

The appropriate distribution warning statement is on the cover page and/or first page and is usually placed in the lower left-hand corner (aligned with left margin), above the classification or handling marking.

# EXHIBIT 6
# SAMPLE OF CNSI MARKINGS




The appropriate classification or handling control is stamped or printed in large font type in ALL CAPS, bold, and centered (left to right) on the top and bottom of all pages.

Recommended font: Arial bold 24 point.

The appropriate distribution warning statements are on the cover page and/or first page. In this sample for CNSI, where two statements are used, the NSI statement is usually placed in the lower left-hand corner (aligned with left margin); the NOFORN statement, in the lower right-hand corner (aligned with right margin). Both statements are above the classification or handling marking.

Recommended font: Arial 8 point.

# EXHIBIT 7
# FILE, EMAIL, APPLICATION/WEBPAGE CONTENT, AND OTHER IT MARKING REQUIREMENTS

1. Printed files, emails, and application/Webpage content shall adhere to requirements for marking hard copy NNPI documents in chapter 2 and exhibit 3. Electronic display of these and other IT items shall adhere to the marking specifications provided below.

2. User notice statements (see chapter 2) for title bars for monitors and display equipment used with NNPI IT equipment and for labels, signs, or notices for IT devices used to print NNPI:

| Classification / Handling | User Notice Statement Options |
|---|---|
| Above SECRET | — None required — |
| SECRET NNPI | "Approved for Classified Use up to SECRET RD & NSI"<br>"Approved for Processing up to SECRET NNPI"<br>"Approved up to SECRET RD & NSI"<br>"Approved up to SECRET NNPI"<br>"SECRET NOFORN" |
| CONFIDENTIAL NNPI | "Approved for Classified Use up to CONFIDENTIAL RD & NSI"<br>"Approved up to CONFIDENTIAL RD & NSI"<br>"Approved up to CONFIDENTIAL NNPI"<br>"CONFIDENTIAL NOFORN"<br>"CONFIDENTIAL" |
| UNCLASSIFIED NNPI | "Approved up to UNCLASSIFIED NNPI" |

3. Electronic NNPI files shall incorporate markings for NNPI in the file name to the maximum extent practical. The first few characters in the file name shall include classification/handling identifier as follows:

| Classification / Handling | Beginning Characters of File Name |
|---|---|
| SECRET Restricted Data | SRD- |
| SECRET National Security Information | SNSI- |
| CONFIDENTIAL Restricted Data | CRD- |
| CONFIDENTIAL National Security Information | CNSI- |
| Not Releasable to Foreign Nationals / UNCLASSIFIED NNPI | UNNPI- |
| UNCLASSIFIED Controlled Nuclear Information | UCNI- |

For example: UNNPI-OPNAVINST.doc

4. On NNPI-accredited information systems: the email address on NNPI authorized exchanges (and the associated display name in directories such as an NNPI global address lists), print queues for NNPI printing, and NNPI

network storage shall include identifiers for NNPI to the maximum extent practical. Generally, NNPI should be part of the name of such items, placed in a consistent location, and discernable to a user of the information system (e.g., NNPI is at the beginning of network storage drive name). Also, <[userid].nnpi@navy.mil> or <[userid]@nnpi.navy.mil> are recommended conventions for the email addresses of NNPI users on NNPI authorized exchanges.

5. At a minimum, application/Webpage content that contains NNPI shall have one of the marking options (see table below), as appropriate for classification/handling, at the top and bottom of the visible screen, and centered left to right. Although distribution warning statements are optional, they should be included if practical to do so, at the bottom of the visible display, but above the classification/handling marking.

6. At a minimum, emails that contain NNPI should have one of the specified marking options (see table below) in the subject line, as well as at the top and bottom of the email body. Distribution warning statements (second column of table) are optional, but should be placed at end of the body of the email above the classification/handling marking, to the maximum extent practical. Guidance (third column of table) may be provided to users, as needed.

| **MARKING** | **DISTRIBUTION WARNING STATEMENT(S)** | **GUIDANCE AND REFERENCE(S) ON APPLICATION AND USE** |
|---|---|---|
| SECRET//RESTRICTED DATA (NNPI)<br>or<br>SECRET – RESTRICTED DATA<br>or<br>SECRET//RD<br>or<br>SECRET–RD<br>or<br>S//RD<br>or<br>SRD<br>or<br>S–RD | Derived from: DOE-DoD classification Guide CG-RN-1<br>Declassify on: Not applicable, no declassification date<br>**RESTRICTED DATA**<br>This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions. | SECRET RESTRICTED DATA (SRD) – A designation applied to classified naval nuclear propulsion information associated with the use of special nuclear material for the production of energy in the nuclear core. Per the Atomic Energy Act of 1954 (as amended), access to SRD requires an investigation on the character, associations, and loyalty of the individual requiring access and subsequent grant of a final (SECRET or higher) Government security clearance.<br><br>SECNAV M-5510.36, DOE-DoD Classification Guide CG-RN-1, and OPNAVINST N9210.3. |
| SECRET//NOFORN (NNPI)<br>or<br>SECRET//NOFORN<br>or<br>SECRET – NOFORN<br>or<br>S//NF<br>or<br>SNF | Derived from: DOE-DoD Classification Guide CG-RN-1<br>Declassify on: 25X4, 25X6; EV.<br>This document shall not be used as a basis for derivative classification guidance.<br><br>**NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command. | SECRET NOFORN – A designation applied to classified naval nuclear propulsion information that is associated with SNSI as defined by EO 13526 (as amended).<br><br>SECNAV M-5510.36, DOE-DoD Classification Guide CG-RN-1, OPNAVINST N9210.3, and CNO ltr 5510 Ser N09N2/8U22301 of 13 May 2008. |

| MARKING | DISTRIBUTION WARNING STATEMENT(S) | GUIDANCE AND REFERENCE(S) ON APPLICATION AND USE |
|---|---|---|
| CONFIDENTIAL//RESTRICTED DATA (NNPI)<br>or<br>CONFIDENTIAL – RESTRICTED DATA<br>or<br>CONFIDENTIAL//RD<br>or<br>CONFIDENTIAL–RD<br>or<br>C//RD<br>or<br>CRD<br>or<br>C–RD | Derived from: DOE-DoD Classification Guide CG-RN-1<br>Declassify on: Not applicable, no declassification date<br>**RESTRICTED DATA**<br>This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions. | CONFIDENTIAL RESTRICTED DATA (CRD) – A designation applied to classified naval nuclear propulsion information associated with the use of special nuclear material for the production of energy in the nuclear core. Per the Atomic Energy Act (as amended), access to CRD requires an investigation on the character, associations, and loyalty of the individual requiring access and subsequent grant of a final (CONFIDENTIAL or higher) Government security clearance.<br><br>SECNAV M-5510.36, DOE-DoD Classification Guide CG-RN-1, and OPNAVINST N9210.3. |
| CONFIDENTIAL//NOFORN (NNPI)<br>or<br>CONFIDENTIAL–NSI (NOFORN)<br>or<br>CONFIDENTIAL – NOFORN<br>or<br>CONFIDENTIAL//NOFORN<br>or<br>C//NF<br>or<br>C–NSI | Derived from: DOE-DoD Classification Guide CG-RN-1<br>Declassify on: 25X4, 25X6; EV.<br>This document shall not be used as a basis for derivative classification guidance.<br><br>**NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command. | CONFIDENTIAL NOFORN – A designation applied to classified naval nuclear propulsion information associated with CNSI as defined by EO 13526 (as amended).<br><br>SECNAV M-5510.36, DOE-DoD Classification Guide CG-RN-1, OPNAVINST N9210.3, and CNO ltr 5510 Ser N09N2/8U22301 of 13 May 2008. |
| NOFORN (U–NNPI)<br>or<br>NOFORN<br>or<br>U//NF | **NOFORN:** This document is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of Naval Sea Systems Command. | NOT RELEASABLE TO FOREIGN NATIONALS (NOFORN) – A designation applied to UNCLASSIFIED naval nuclear propulsion information (U-NNPI), which is unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.<br><br>OPNAVINST N9210.3 and CNO ltr 5510 Ser N09N2/ 8U22301 of 13 May 2008. |

| MARKING | DISTRIBUTION WARNING STATEMENT(S) | GUIDANCE AND REFERENCE(S) ON APPLICATION AND USE |
|---|---|---|
| UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION<br>or<br>UCNI | **UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION:** Not for public dissemination. Unauthorized dissemination is subject to civil and criminal sanctions under Sec. 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168). | UNCLASSIFIED Controlled Nuclear Information (UCNI) – A designation applied to information under DOE jurisdiction that includes UNCLASSIFIED facility design information; operational information concerning the production, processing, or use of nuclear material for atomic energy defense programs; safeguards and security information; and nuclear material.<br><br>OPNAVINST N9210.3. |