NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2026.1

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Safeguarding of Naval Nuclear Propulsion Information (NNPI) (2010)**

Focal Document URL: https://www.secnav.navy.mil/doni/Directives/09000%20General%20Ship%20Design%20and%20Support/09-200%20Propulsion%20Plants%20Support/N9210.3%20(Unclas%20Portion).pdf

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-usa-federal-dow-safeguarding-nnpi-2010.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
CHAPTER 1	DEFINITION	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-1	Definition	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-2	Guidance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-2.a	Guidance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-2.b	Guidance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3	NNPI Determination	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.a	NNPI Determination	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b	NNPI Determination	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(1)	NNPI Determination	A naval nuclear propulsion plant or support facility application is directly referred to by any of the following:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(1)(a)	NNPI Determination	Ship name or hull number.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(1)(b)	NNPI Determination	Project designator.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(1)(c)	NNPI Determination	Ship system identification.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(1)(d)	NNPI Determination	Component nameplate data.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(1)(e)	NNPI Determination	Component name revealing a reactor plant function.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(2)	NNPI Determination	A system or component listed in table 2.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.b(3)	NNPI Determination	Details on technical parameters or operational conditions (e.g., design temperature or pressure).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.c	NNPI Determination	Items or information specifically identified by CNO (N00N) as NNPI shall be marked and handled as such.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.d	NNPI Determination	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):	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.d(1)	NNPI Determination	It is available "commercial off-the-shelf."	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.d(2)	NNPI Determination	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.d(3)	NNPI Determination	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.).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-3.d(4)	NNPI Determination	It meets other exemption criteria as determined by CNO (N00N).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-4	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1-5	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).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 2	MARKING	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-2	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)).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-3	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-4	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-5	Paragraph and Portion Markings	Paragraph or portion markings are not required for NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-6	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.a	IT media	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-7.a(1)	IT media	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.a(2)	IT media	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.a(3)	IT media	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).	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.b(1)	U-NNPI IT equipment.	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-7.b(1)(a)	U-NNPI IT equipment.	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.b(1)(b)	U-NNPI IT equipment.	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.b(2)	Classified NNPI IT equipment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2-7.b(2)(a)	Classified NNPI IT equipment	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.b(2)(b)	Classified NNPI IT equipment	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.c	Electronic display	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2-7.c(1)	Electronic display	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.c(2)	Electronic display	Monitors and display equipment used for NNPIauthorized IT equipment shall have a title bar on the screen identifying authorization for NNPI.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.c(2)(a)	Electronic display	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.c(2)(b)	Electronic display	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.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
2-7.c(2)(c)	Electronic display	Mobile devices approved for NNPI shall have the appropriate title bar to the maximum extent practical.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
CHAPTER 3	CONTROL AND STORAGE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3-2	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3-3	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3-4	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).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3-5	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 4	DISCLOSURE POLICY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-2	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-3	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-4	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-5	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-6	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-7	Contractors and Subcontractors	These requirements are addressed in chapter 7.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4-8	Unauthorized Release	Any release of NNPI in violation of the disclosure policy outlined in this chapter shall be reported to CNO (N00N).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 5	PUBLIC RELEASE	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5-2	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5-3	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 6	DISPOSAL	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-1	Documents	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-1.a	Disposal	NNPI documents shall be disposed as classified material.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
6-1.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.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
6-1.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).	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
6-2	Components and Equipment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-2.a	Components and Equipment	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.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
6-2.b	Components and Equipment	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-2.c	Components and Equipment	Unless specifically authorized by a ship alteration or other NAVSEASYSCOM correspondence, reactor plant components assigned 25 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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-2.d	Components and Equipment	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 nuclearunique 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).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-2.e	Components and Equipment	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6-2.f	Components and Equipment	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
6-3	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.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
6-3.a	Disposal of IT Equipment and Media	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.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
6-3.b	Disposal of IT Equipment and Media	Classified NNPI materials must be disposed of under National Security Agency (NSA) requirements for classified material.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
CHAPTER 7	CONTRACTORS AND SUBCONTRACTORS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7-2	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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7-2	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.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
7-3	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 UNNPI until subsequent contractual controls are established. Appendix C is a sample stipulation.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7-4	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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7-4	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.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
7-5	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.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
7-5	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.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
CHAPTER 8	FACILITY VISITS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8-2	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8-3	Foreign Nationals or Representatives of a Foreign Interest	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8-3.a	Foreign Nationals or Representatives of a Foreign Interest	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.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
8-3.a(1)	Foreign Nationals or Representatives of a Foreign Interest	The visitor(s) shall be kept under close and continuous surveillance at all times while within the physical confines of the facility.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
8-3.a(2)	Foreign Nationals or Representatives of a Foreign Interest	Visual, oral, and documentary disclosures of NNPI shall be prevented by isolating areas, materials, or personnel.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	5	
8-3.a(2)	Foreign Nationals or Representatives of a Foreign Interest	Visual, oral, and documentary disclosures of NNPI shall be prevented by isolating areas, materials, or personnel.	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
8-3.a(3)	Foreign Nationals or Representatives of a Foreign Interest	The visit shall be accomplished without adverse impact on the facility's workload, scheduling, or other key management factors.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
8-3.b	Foreign Nationals or Representatives of a Foreign Interest	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8-3.c	Foreign Nationals or Representatives of a Foreign Interest	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 9	INFORMATION TECHNOLOGY (IT) POLICY	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9-2	Requirements	NNPI shall be safeguarded on IT systems.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
9-2	Requirements	NNPI shall be safeguarded on IT systems.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
9-2.a	Requirements	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.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
9-2.a	Requirements	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.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	8	
9-2.b	Requirements	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.	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
9-2.b	Requirements	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.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
9-2.b	Requirements	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.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	8	
9-2.b	Requirements	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.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	8	
9-2.b	Requirements	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.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	8	
9-2.b	Requirements	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.	Functional	Intersects With	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications, Services and/or Data (TAASD) under their control on an ongoing basis for applicable threats and risks, as well as to ensure security, compliance and resilience controls are operating as intended.	8	
9-2.c	Requirements	IT systems used for NNPI should be marked/labeled following chapter 2 specifications for IT equipment, IT media, and electronic display.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
9-2.d	Requirements	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).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8	
9-2.e	Requirements	Responsibilities for implementing, controlling, and protecting NNPI on IT systems are assigned in chapter 10.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
9-3	Restrictions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9-3.a	Restrictions	NNPI may only be authorized for IT systems owned or operated by, for, or on behalf of an NNPP activity.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
9-3.b	Restrictions	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.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
9-3.c	Restrictions	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.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	3	
9-3.c	Restrictions	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.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	3	
9-3.d	Restrictions	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.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	5	
9-3.d	Restrictions	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.	Functional	Intersects With	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5	
9-3.e	Restrictions	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.	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
9-4	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).	Functional	Intersects With	Sensitive / Regulated Data Spill Response	IRO-12	Mechanisms exist to respond to sensitive/regulated data spills.	5	
9-5	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.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
9-6	Contact	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 10	INFORMATION TECHNOLOGY (IT) RESPONSIBILITIES	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-2	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-2.a	Information Owner	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-2.b	Information Owner	Under CNO (N00N)'s statutory authority, the DCS shall oversee cases of improper handling of NNPI and support the DAA investigations involving NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-2.c	Information Owner	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3	DAA	The DAA formally assumes the responsibility for operating an IT system at an acceptable level of risk.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.a	DAA	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.a(1)	DAA	Reference (h) authorizes the CO of a Navy vessel operating at sea to serve as a deployed DAA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.a(2)	DAA	Echelon 2 headquarters organizations may function as the DAA for research, development, test, and evaluation (RDT&E) networks as prescribed in reference (h).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.a(3)	DAA	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.a(4)	DAA	Defense Security Service is the DAA for classified information systems owned or operated by, for, or on behalf of the vendors supporting the Navy.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.b	DAA	DAAs with overlapping responsibilities shall resolve any conflicts by formal written agreement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c	DAA	NAVNETWARCOM and echelon 2 RDT&E DAAs shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(1)	DAA	Accredit IT systems for NNPI per CNO (N00N) assessment:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(1)(a)	DAA	Incorporate CNO (N00N) review and concurrence into the C&A of systems that process (or are planned to process) NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(1)(b)	DAA	Obtain CNO (N00N) concurrence for NNPI processing before issuing an authorization (e.g., authorization to operate) for an IT system to process NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(2)	DAA	Address unauthorized disclosures of NNPI:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(2)(a)	DAA	Inform CNO (N00N) of any potential, alleged, or actual compromise of NNPI on IT systems	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(2)(b)	DAA	Develop and maintain systems and processes to report, respond, track, and resolve unauthorized disclosures or improper handling of NNPI on IT systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(2)(c)	DAA	Work to minimize the unauthorized disclosures of NNPI and to mitigate their impacts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(2)(d)	DAA	Assist in investigating the improper handling of NNPI on IT systems by providing technical experts.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(2)(e)	DAA	Coordinate the mitigation and remediation strategy for any compromise of NNPI on IT systems not authorized to process NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(3)	DAA	Include CNO (N00N) in IT infrastructure strategy and planning involving NNPI systems and support audits and reviews:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(3)(a)	DAA	Provide (or coordinate) access to personnel and training material associated with NNPI at the IT system operation centers, facilities, or support locations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(3)(b)	DAA	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(4)	DAA	Serve as the primary point of contact on information assurance (IA) issues with IT systems processing NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(5)	DAA	Consult CNO (N00N) on requirements for NNPI, such as:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(5)(a)	DAA	Providing CNO (N00N) a copy of all inquiries regarding NNPI protections and a copy of the proposed response for concurrence before issuing the response.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-3.c(5)(b)	DAA	Consulting with CNO (N00N) on clarifications to Navy requirements for the protection of NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-4	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.a	Program Manager	Adhere to requirements for safeguarding NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.b	Program Manager	Incorporate NNPI protections into baseline requirements for IT systems that process or are planned to process NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.c	Program Manager	Include CNO (N00N) in discussions or reviews required to clarify the proper safeguarding of NNPI on IT systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.d	Program Manager	Include CNO (N00N) in discussions or reviews on IT systems and the IT services or capabilities NNPP needs.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.e	Program Manager	Coordinate with the cognizant DAA, CNO (N00N), and CA personnel to properly test and evaluate systems and services involving NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.f	Program Manager	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-5.g	Program Manager	Develop work processes to track and maintain formal communication with CNO (N00N) on IT systems containing NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-6	Commanding Officer/Officer in Charge (CO/OIC)	Per reference (i), the CO/OIC shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-6.a	Commanding Officer/Officer in Charge (CO/OIC)	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-6.b	Commanding Officer/Officer in Charge (CO/OIC)	Ensure that personnel under their command are trained in and abide by IA policy, including NNPI control and protection requirements.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-6.c	Commanding Officer/Officer in Charge (CO/OIC)	Ensure that all IT assets they oversee and operate are accredited and operated in keeping with the C&A documentation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-6.d	Commanding Officer/Officer in Charge (CO/OIC)	Designate an NNPICO (per chapter 2 of this instruction) for activities processing NNPI on IT systems.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-6.e	Commanding Officer/Officer in Charge (CO/OIC)	Appoint agents, as necessary, to review records associated with NNPI matters at the Navy network operation centers, facilities, or support locations.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-7	Information Assurance Manager (IAM)	Per reference (i), the IAM is responsible for IA within a command, site, or system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-7.a	Information Assurance Manager (IAM)	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
10-7.b	Information Assurance Manager (IAM)	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-7.c	Information Assurance Manager (IAM)	IAMs will inform CO/OICs, NAVNETWARCOM, and CNO (N00N) of all NNPI incidents on Navy IT systems involving their command. For example:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-7.c(1)	Information Assurance Manager (IAM)	All inquiries regarding NNPI issues.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-7.c(2)	Information Assurance Manager (IAM)	Actual, potential, or alleged mishandling of NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-7.c(3)	Information Assurance Manager (IAM)	Navy IT system vulnerabilities involving risk of unauthorized access to NNPI.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-8	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10-9	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 11	INFORMATION SYSTEMS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-2	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).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
11-3	Information Systems	Per reference (h), information systems not designated as PIT shall be certified and accredited by the Navy DAA.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a	Information Systems	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(1)	Information Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(2)	Information Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(2)(a)	Information Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(2)(b)	Information Systems	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(2)(b)1	Information Systems	The applicable requirements in OPNAV 9210/1.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(2)(b)2	Information Systems	The selected control(s), from either reference (n) or reference (q), for each requirement.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(2)(b)3	Information Systems	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.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	5	
11-3.a(3)	Information Systems	In DIACAP phase 3 (Make Certification Determination and Accreditation Decision):	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(3)(a)	Information Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(3)(b)	Information Systems	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).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(3)(c)	Information Systems	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.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
11-3.a(4)	Information Systems	In DIACAP phase 4 (Maintain ATO and Conduct Reviews), the IAM shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(4)(a)	Information Systems	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.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
11-3.a(4)(b)	Information Systems	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.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
11-3.a(4)(c)	Information Systems	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.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
11-3.a(4)(d)	Information Systems	Ensure disposal or disposition of components of the information system determined to contain or possibly contain NNPI per chapter 6 this instruction.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11-3.a(5)	Information Systems	In DIACAP phase 5 (Decommissioning), the IAM shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.a(5)(a)	Information Systems	Ensure that any significant NNPI security control inheritance relationships are resolved before decommissioning the information system.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
11-3.a(5)(b)	Information Systems	Remove OPNAV 9210/1 and supporting detailed documentation on NNPI security control implementation for the information system from all tracking systems.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
11-3.a(5)(c)	Information Systems	Ensure disposal or disposition of components of the information system determined to contain or potentially contain NNPI per chapter 6 this instruction.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11-3.b	Information Systems	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.b(1)	Information Systems	The IAM shall incorporate this instruction, including table 3, into the information system security requirements as discussed in subparagraph 3a(1) of this chapter.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.b(2)	Information Systems	The IAM shall work with the PM to implement necessary changes to the information system to meet the revised NNPI requirements in this instruction.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
11-3.b(3)	Information Systems	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.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that:(1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS);(2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and(3) Provides a historical record of applied security controls, including changes.	5	
11-3.b(4)	Information Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-3.c	Information Systems	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.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
11-4	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-4.a	User Authorization	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-4.b	User Authorization	Signature of a supervisor attesting to the user's NTK for NNPI in the performance of assigned duties and responsibilities.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-4.c	User Authorization	Acceptance by the user of IA responsibilities for NNPI on the Navy information system.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11-5	Transport	Transporting NNPI-related information systems outside the United States or its territories requires CNO (N00N) approval.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	3	
11-5.a	Transport	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).	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	3	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
11-5.b	Transport	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.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	3	
11-6	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.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
CHAPTER 12	TELECOMMUNICATION SYSTEMS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-1	General	See FDE for details.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2	Telecommunication Systems	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.a	Telecommunication Systems	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.	Functional	Intersects With	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	3	
12-2.b	Telecommunication Systems	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.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
12-2.c	Telecommunication Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.d	Telecommunication Systems	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.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
12-2.e	Telecommunication Systems	U-NNPI-related telecommunications in areas outside the United States or its territories shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.e(1)	Telecommunication Systems	Use Federal Information Protection Standard (FIPS) 140-2 certified or NSA type-1 encryption for all transmissions between end-points.	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
12-2.e(2)	Telecommunication Systems	Take place over devices issued, owned, or leased by an NNPP activity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.e(3)	Telecommunication Systems	Be conducted over lines (or channels, such as cellular) owned or leased by an NNPP activity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.e(4)	Telecommunication Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f	Telecommunication Systems	U-NNPI-related telecommunications in areas within the United States or its territories shall:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(1)	Telecommunication Systems	For U-NNPI voice and fax:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(1)(a)	Telecommunication Systems	Take place over devices issued, owned, or leased by an NNPP activity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(1)(b)	Telecommunication Systems	Be conducted over lines (or channels, such as cellular) owned or leased by an NNPP activity.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(1)(c)	Telecommunication Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(2)	Telecommunication Systems	For U-NNPI VTC, follow the requirements provided in subparagraph 2e of this chapter.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)	Telecommunication Systems	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:	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)(a)	Telecommunication Systems	The device is not connected (wired, wireless, or other) to a computer (desktop, laptop, mobile, or other).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)(b)	Telecommunication Systems	Voice, video, photography, or faxes are not saved to any non-volatile storage within, attached, or connected to the device.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)(c)	Telecommunication Systems	Temporary storage is not retransmitted.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)(d)	Telecommunication Systems	The device does not use image-retaining print mechanisms (such as carbon or ink ribbon).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)(e)	Telecommunication Systems	Transcribing/conversion features or capabilities (such as voice to text) are not in operation.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-2.f(3)(f)	Telecommunication Systems	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-3	Transport	Transporting NNPI-related telecommunication systems to locations outside the United States or its territories requires CNO (N00N) approval.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-3.a	Transport	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).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-3.b	Transport	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12-4	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
CHAPTER 13	OTHER ELECTRONICS	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-1	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).	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-2	Other Electronics	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-2.a	Other Electronics	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-2.b	Other Electronics	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-2.b(1)	Other Electronics	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-2.b(2)	Other Electronics	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.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
13-3	Transport	Transporting NNPI-related electronics addressed by this chapter to locations outside the United States or its territories requires CNO (N00N) approval.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
13-3.a	Transport	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).	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
13-3.b	Transport	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.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13-4	Deviations	Waivers for any of the above requirements involving NNPI must be formally submitted to CNO (N00N) for approval.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	