Safeguarding Controlled Unclassified Information & Naval Nuclear Propulsion Information

Newport News Shipbuilding
A Division of HII

Jessica Borst

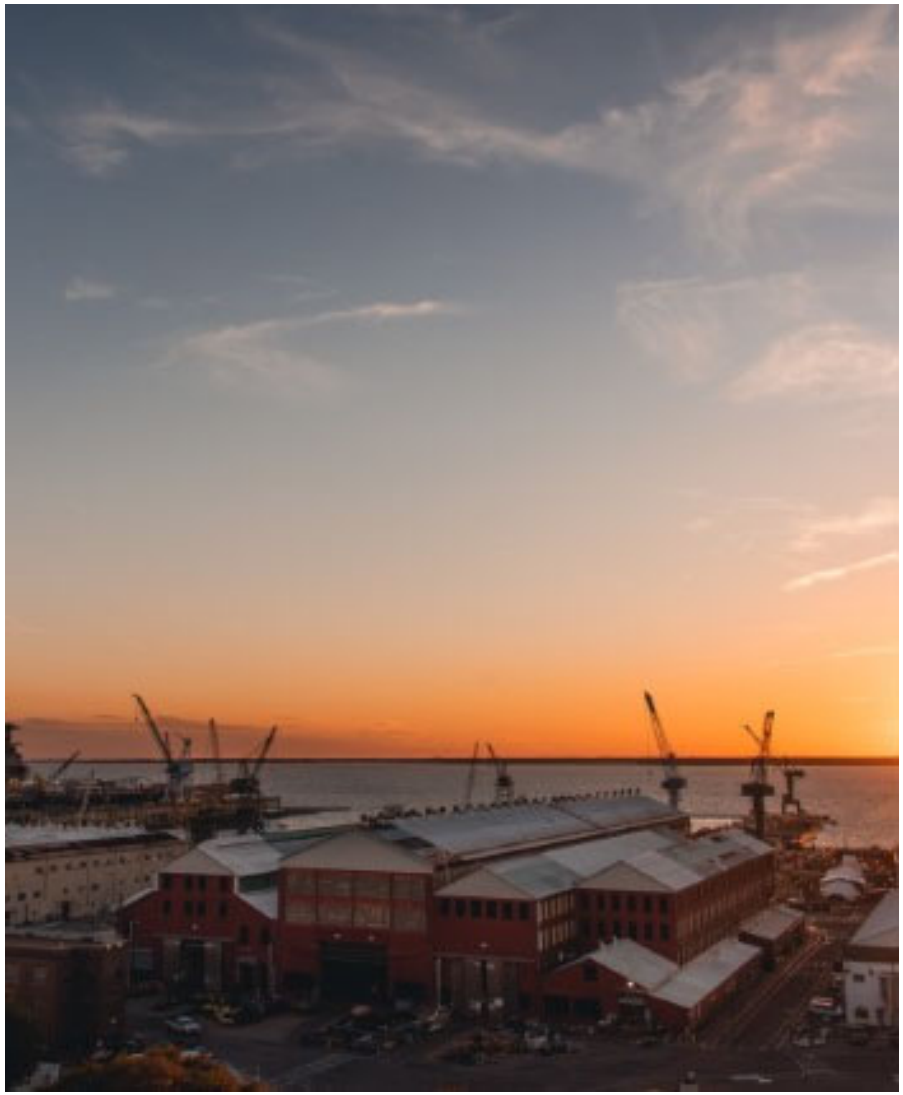
October 25-27, 2022

Housekeeping

We have all attendees joined on mute.

As we go through the presentation, please submit questions via the chat box to the panelists and we will address them during pauses throughout the webinar.

Thank you for attending!



Safeguarding Information

Purchase Orders may involve the distribution and receiving of information that must be protected. Two common forms of information distributed or received by NNS are:

- Controlled Unclassified Information (CUI)
- Naval Nuclear Propulsion Information (NNPI)

NNPI is a sub-set of CUI with stricter requirements, as outlined in OPNAV N9210.3.

Agenda

CUI and NNPI Topics

- What are they?
- How NNS transmits the controlled information
- Process to receive from NNS electronically
- Control, storage, transmission, disposal and destruction of Controlled Information
- For NNPI: additional req's on transmission and OPNAV N9210.3

Safeguarding Controlled Unclassified Information

Newport News Shipbuilding

A Division of HII

What Is Controlled Unclassified Information (CUI)?

Any information that is:

Created or possessed by the government

OR

Created by a Supplier for or on behalf of the government

AND

Subject to safeguarding and/or dissemination controls stipulated by law, regulation, or government-wide policy.

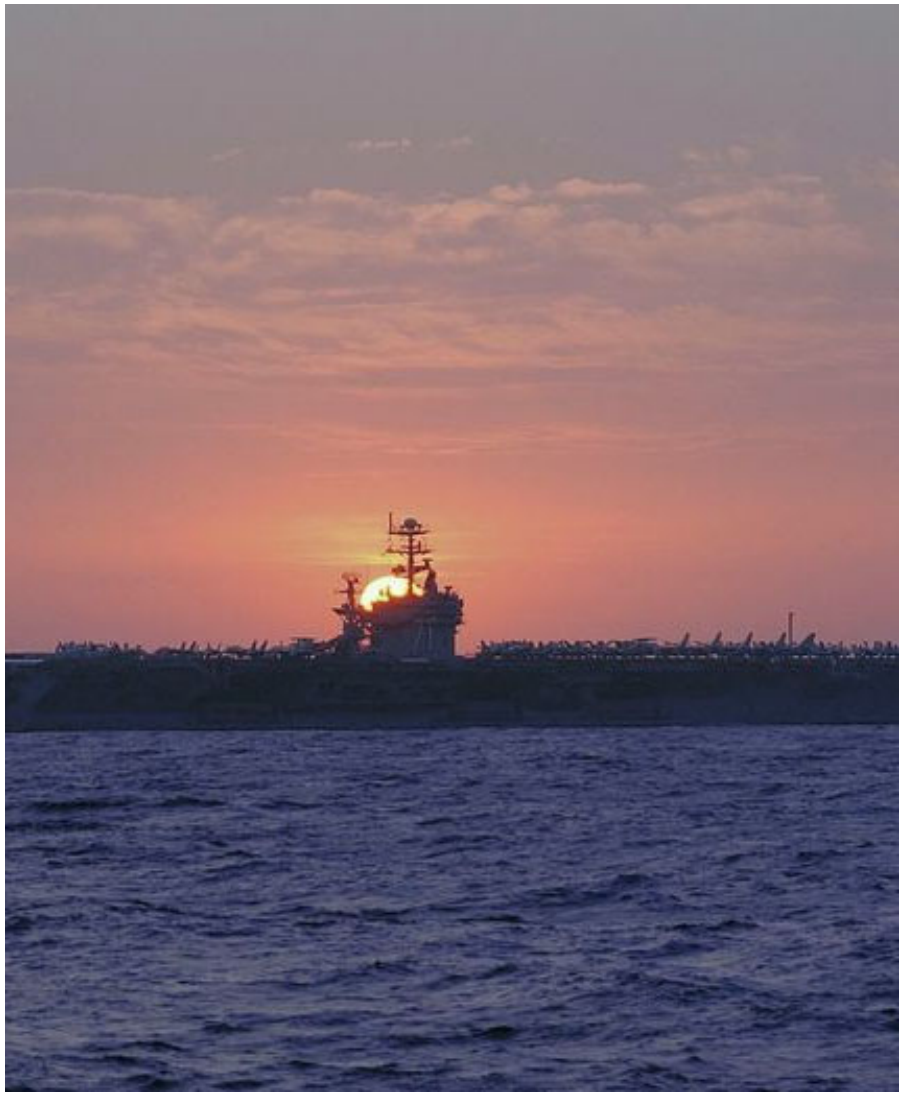
Safeguarded Information Matrix - CUI

The below matrix outlines requirements for how CUI is transmitted to our suppliers. We will go into additional details for CUI in the following slides.

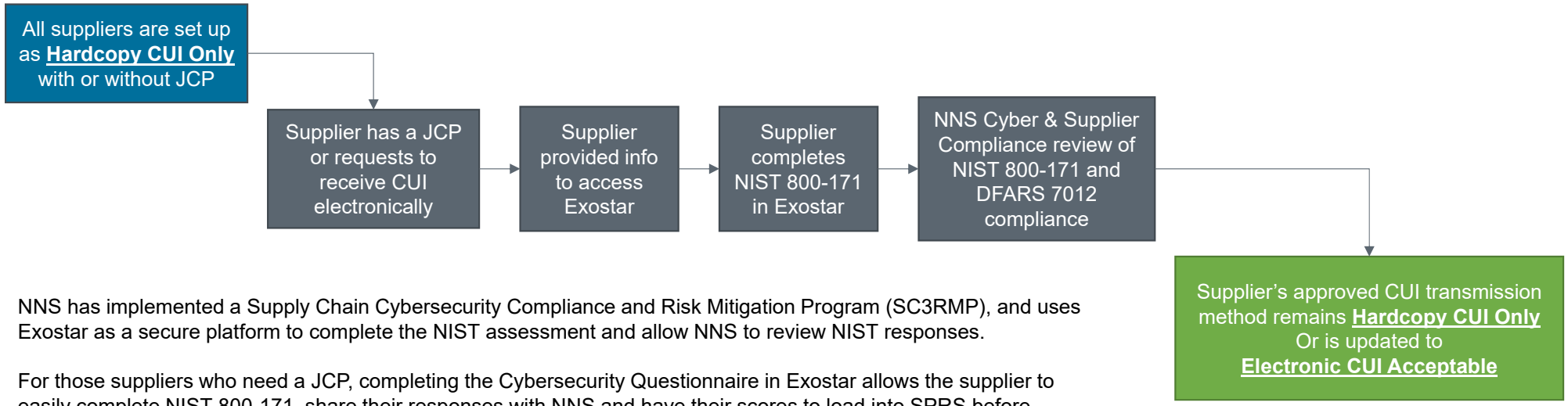
CUI Category or Document Marking	NIST 800-171	JCP	Transmission Types	Electronic Transmission Requirements	Approved Transmission
CUI // Procure Obsolete legacy markings: FOUO, OUO, SBU	Not required for Hardcopy CUI; Required for Electronic CUI Transmission Approval	No	Hardcopy CUI Only **or** Electronic CUI Acceptable	Electronic CUI Acceptable is conditional upon NIST 800-171 completion and Cybersecurity/Supply Chain evaluation	Can be shared in accordance with supplier's approved CUI transmission method
CUI // CTI CUI // EXPT Obsolete legacy markings: Distribution Statements B-F	Required for JCP Registration	Yes	Without JCP: None With JCP: Hardcopy CUI Only **or** Electronic CUI Acceptable	Electronic CUI Acceptable is conditional upon NIST 800-171 completion and Cybersecurity/Supply Chain evaluation	If no JCP, cannot be shared with supplier! If JCP, can be shared in accordance with supplier's approved CUI transmission method

How Buyers will transmit CUI to our NNS Suppliers:

- **Hardcopy CUI**:
  - CUI may be sent to Stand-alone fax machines
    - Faxed within the US and its territories provided there is an authorized person waiting to receive the document and properly control it; **AND**
    - Provided the receiving device is not connected to a computer)
  - Physically mailed after confirming recipient's need-to-know (NTK) and mailing address, with no markings that would indicate sensitivity of contents
- **Electronic CUI Acceptable**:
  - Exostar Information Manager application
  - Email Encryption employing FIPS 140-2 data-at-rest encryption
  - Fax machines to include networked
  - Hardcopy CUI transmission methods listed above



Supplier Process for Evaluation to Receive Electronic CUI



NNS has implemented a Supply Chain Cybersecurity Compliance and Risk Mitigation Program (SC3RMP), and uses Exostar as a secure platform to complete the NIST assessment and allow NNS to review NIST responses.

For those suppliers who need a JCP, completing the Cybersecurity Questionnaire in Exostar allows the supplier to easily complete NIST 800-171, share their responses with NNS and have their scores to load into SPRS before submitting the JCP application.

Contact Exostar@hii-nns.com to assist with getting access to Exostar's application for completing the NIST questionnaire.

JCP Requirements for suppliers receiving CUI // CTI, CUI // EXPT, or Legacy Markings: Distribution Statements B-F

Active Commercial and Government Entity (CAGE) Code

Current System for Award Management (SAM) registration

Load NIST 800-171 into SPRS

Complete DD Form 2345 (JCP application)

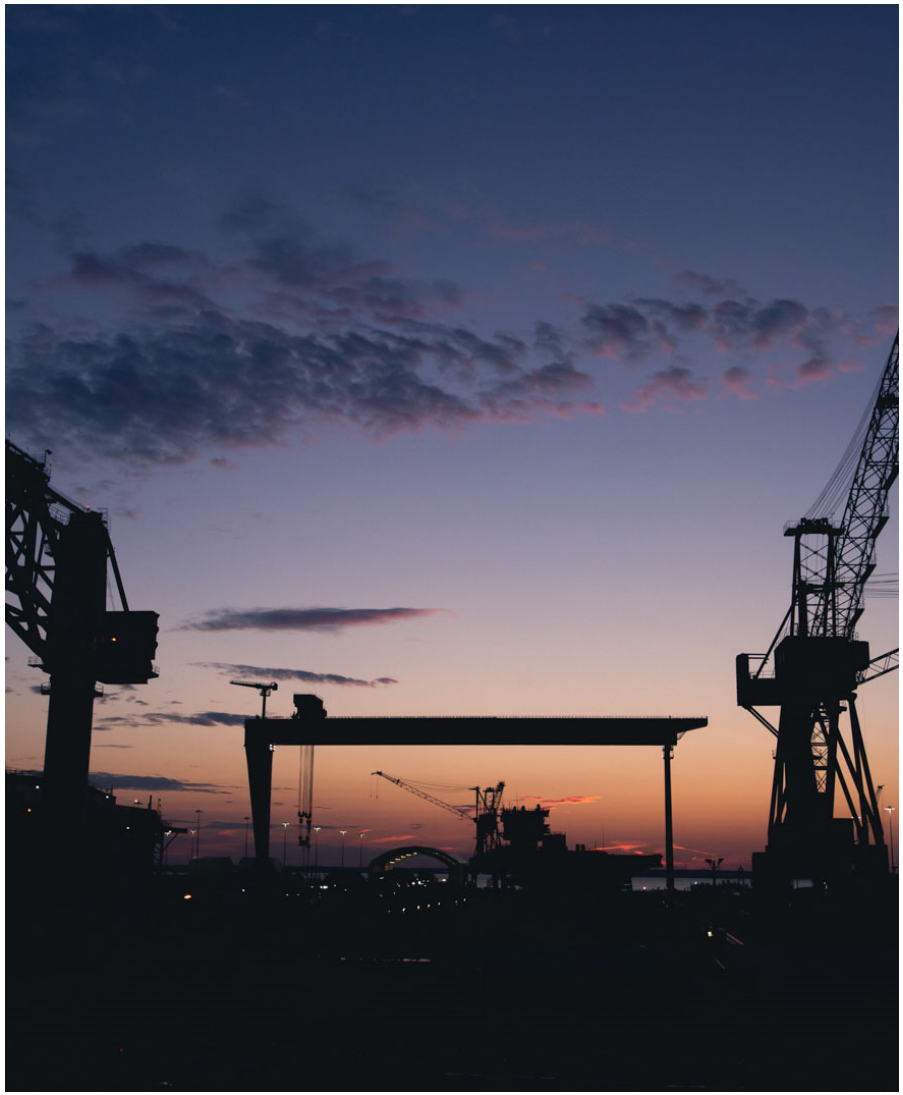
Submit JCP Application to DLA

JCP Home (dla.mil)

Note: *This slide is intended as a snapshot overview of requirements outlined on the DLA's website and does not negate compliance with any additional requirements outlined by DLA.*

CUI Control – When in Use

- CUI shall be controlled so that those without authorized access & a NTK cannot obtain visual or physical access that would permit detailed examination.
- Prevent CUI exposure to foreign nationals.
- CUI materials should be put away, covered, or turned face-down anytime persons without NTK are present.

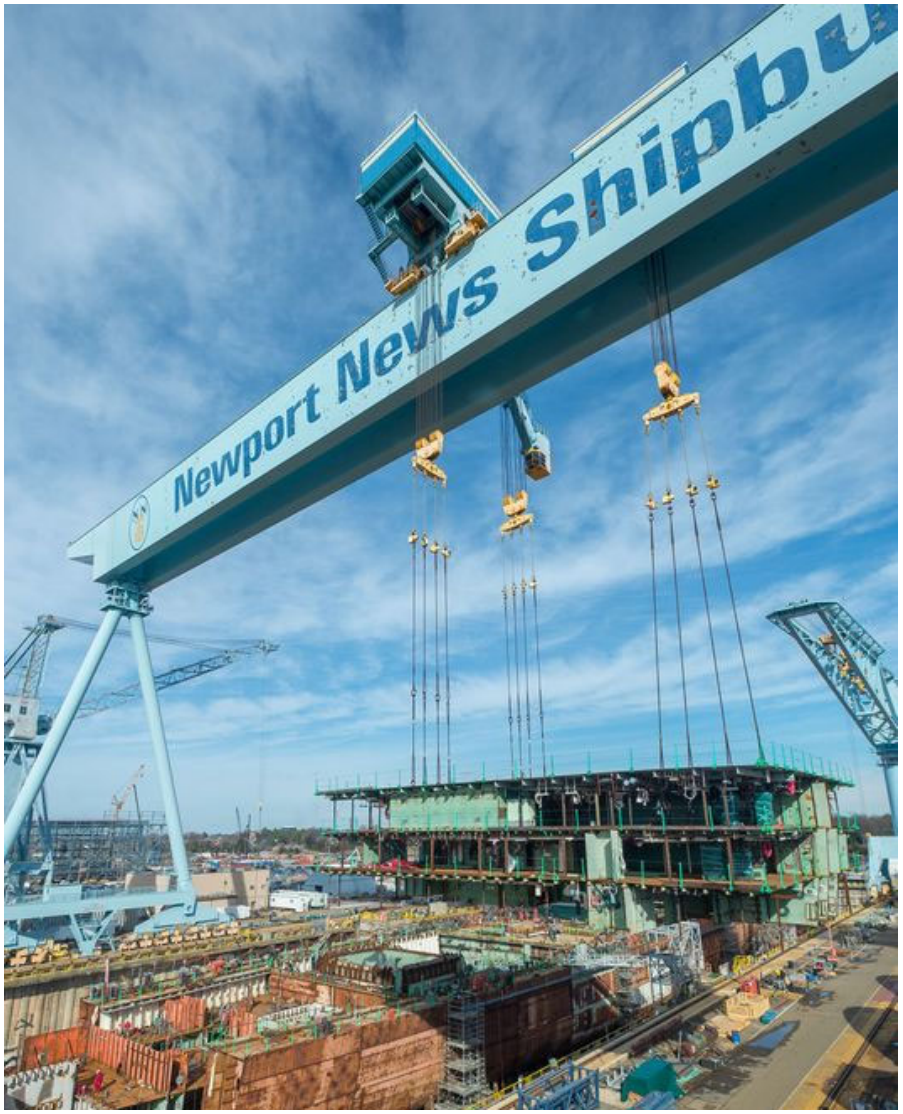


CUI Storage

- Safeguard by storing it in a controlled environment with physical and/or procedural controls sufficient to prevent unauthorized access.
- Any authorized or accredited measures for safeguarding classified information are also sufficient for safeguarding CUI.
- Safeguarding CUI requires a sturdy container or designated room or closet that:
  - Is secured by a key-operated lock
  - Shows immediate signs of tampering to access

CUI Disposal & Destruction

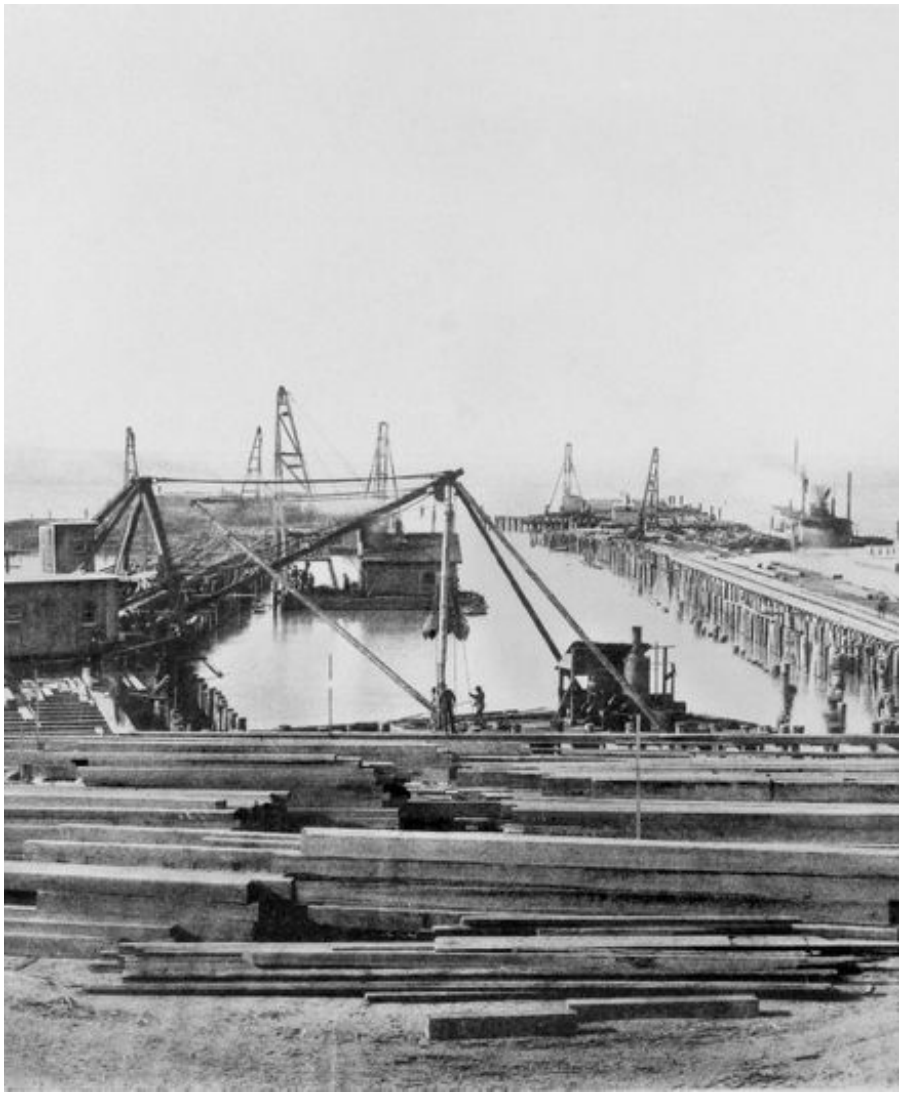
- Unless NNS authorizes retention by the supplier, CUI documents or media no longer required for contract execution shall be:
  - Securely returned to NNS; or
  - Destroyed using means that will prevent reconstruction of the document



Points of Contact

Questions?

- NNS NNPI Control Officer
  - Stephen Simmons
  - Office: (757) 688-5287
  - Stephen.Simmons@hii-nns.com
- NNS Supplier Data team
  - NNSSupplierData@HII-NNS.com
- HII Exostar Team
  - Exostar@hii-nns.com
- HII External Supplier Website
  - https://supplier.huntingtoningalls.com



Safeguarding Naval Nuclear Propulsion Information

Newport News Shipbuilding

A Division of HII

What Is Naval Nuclear Propulsion Information (NNPI)?

NNPI is 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.

OPNAVINST N9210.3

- Guidance document for NNPI protections
- Guidance is 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.
- Contains definitions, marking requirements, safeguarding and storage requirements, disclosure policy and restrictions, facility visits, etc.

Training is intended as an overview of requirements and does not negate compliance with all applicable sections in the above guidance document.

Safeguarded Information Matrix - NNPI

The below matrix outlines requirements for how NNPI is transmitted to our suppliers. We will go into additional details for NNPI in the following slides.

CUI Category or Document Marking	NIST 800-171	JCP	NN9540	Transmission Types	Electronic Transmission Requirements	Approved Transmission
CUI // NNPI	Required for JCP Registration	Yes	Yes	Without JCP and NN9540 Form: None With JCP and NN9540 Form: Hardcopy NNPI Only **or** Electronic NNPI Acceptable	Electronic NNPI Acceptable is conditional upon receipt of NAVSEA08 ATO letter.	If no JCP and NN9540 Form, cannot be shared with supplier! If JCP and NN9540 Form, can be shared in accordance with supplier's approved NNPI transmission method.

Note: Electronic CUI Acceptable does not mean Electronic NNPI Approved! The NAVSEA08 ATO letter is REQUIRED to receive Electronic NNPI transmissions.

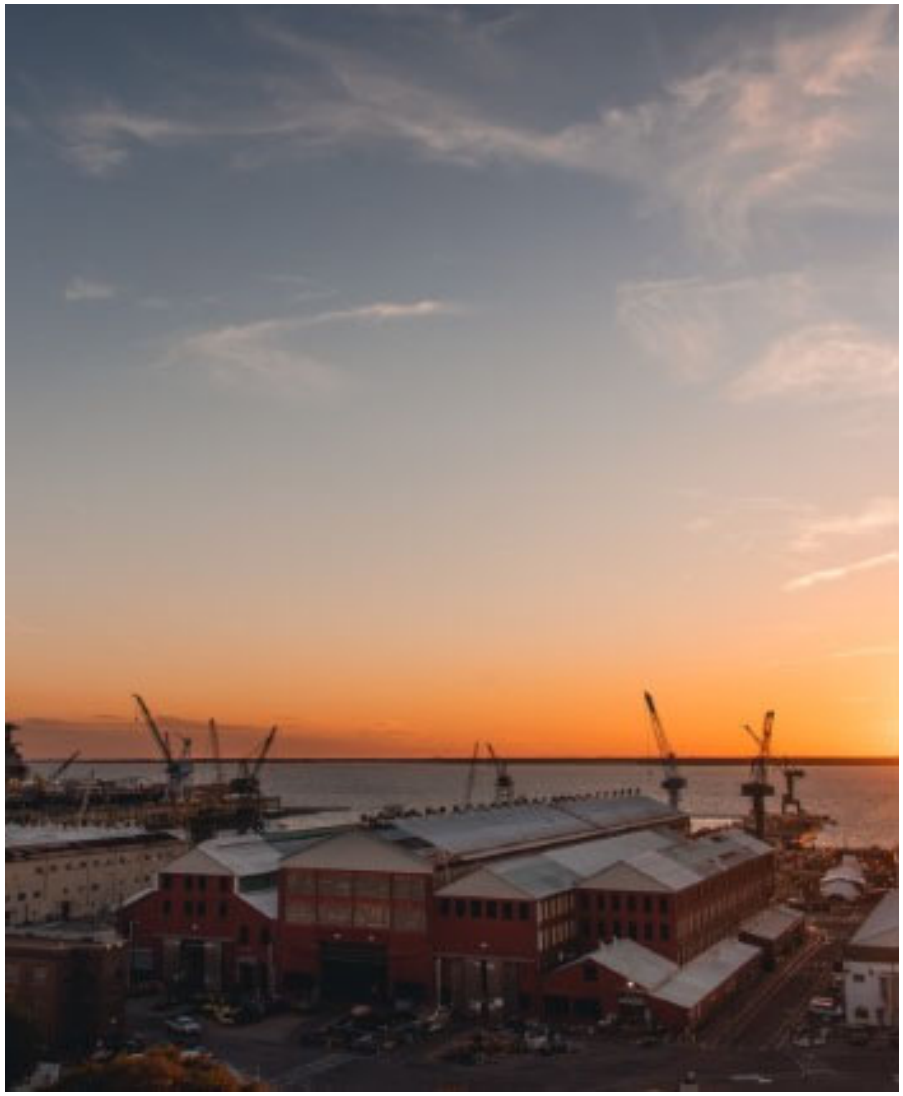
How Buyers will transmit NNPI to our NNS Suppliers:

- NNPI may be sent to Stand-alone fax machines
  - Faxed within the US and its territories provided there is an authorized person waiting to receive the document and properly control it; **AND**
  - Provided the receiving device is not connected to a computer)

- NNPI may not be faxed outside of the US or its territories, unless the transmission line is encrypted using a means approved by NAVSEA 08 Cybersecurity

How Buyers will transmit NNPI to our NNS Suppliers:

- NNPI may be shipped within the US and its territories via Certified Mail.
- The buyer may reach out to validate the supplier's address immediately before sending.
- The material must be addressed to a specific person who is known to have valid citizenship and NTK.
- NNPI will be shipped in an opaque envelope/package that bears no external markings indicating the sensitivity of the contents.

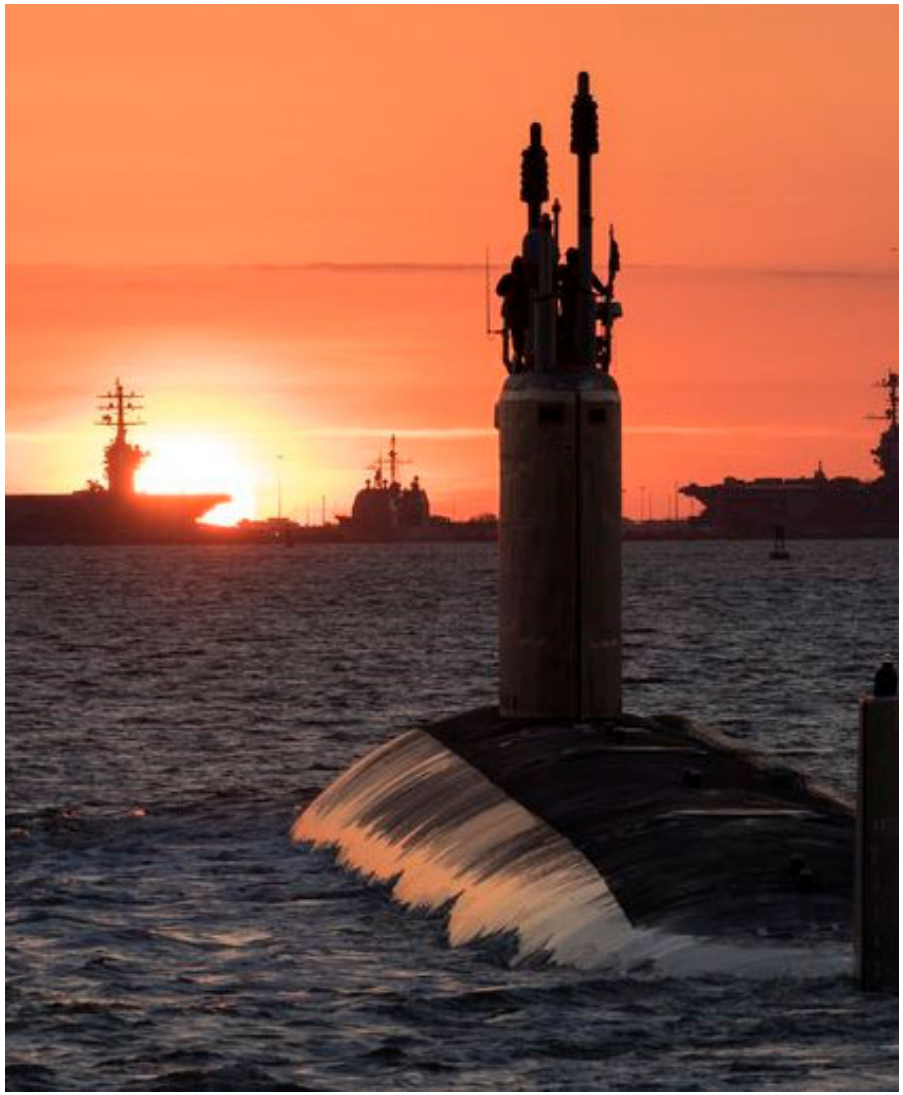


NNPI Authorized Computers

- NNPI may not be processed or stored on a Supplier-owned computer system or portable electronic device unless authorized by NAVSEA 08 Cybersecurity. NNPI may only be transmitted via the Internet to NAVSEA-approved computer systems.
  - S/MIME encryption is required
  - Ensure NNS Supplier Data team has the NAVSEA 08 "Authorization to Operate" (ATO) in order to receive 'electronic' transmission of NNPI
- Any removable media (thumb drives, CDs/DVDs, etc.) or external drives containing NNPI must be encrypted to FIPS 140-2 standards and must bear markings similar to those required for printed documents containing the same information. **Again, for this to apply … you must have the NAVSEA08 Cybersecurity Authority to Operate.**

Supplier-Originated NNPI Documents

- Supplier-originated documents that reproduce, expand upon, or modify information drawn from NNPI documents must have the **NOFORN** marking at the top and bottom of every page.
- The following warning statement must appear on a cover sheet or displayed on the first page:
  - 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.



NNPI Control – When in Use

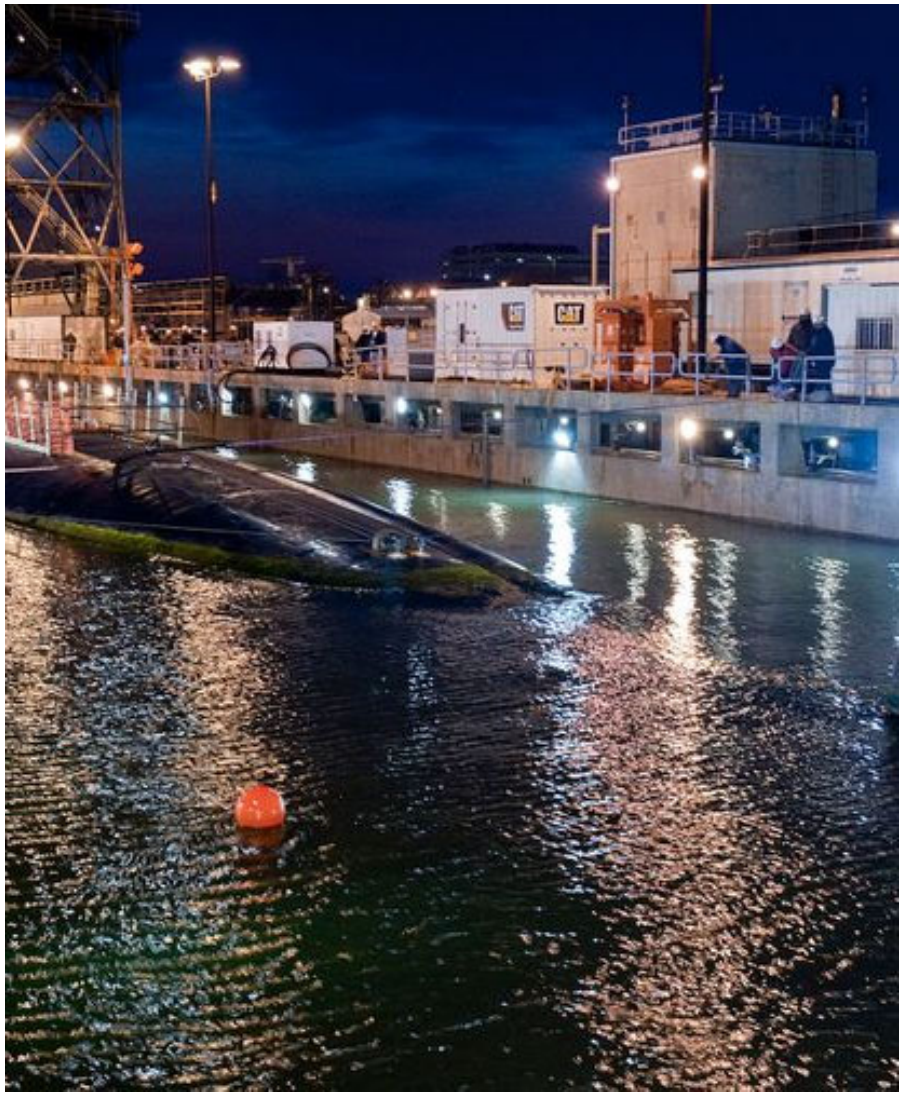
- NNPI must be controlled so that those without authorized access & a NTK cannot obtain visual or physical access.
  - Authorized access – U.S. citizens or U.S. nationals with a valid NTK.
  - Unauthorized access – Resident Aliens ("green card" holders) is prohibited.
  - NAVSEA 08 Security must be notified before granting any Dual citizen access to NNPI.
- When NNPI documents are in the custody of an authorized individual using them, it must remain under their direct physical control and in their personal possession.
  - Must never be left unsecured, sent with checked baggage, or left unattended in an automobile or hotel room.

NNPI Control – When in Use

- **NNPI hardware being produced must also be safeguarded!**
- Access to the space(s) where the hardware is produced/stored must be restricted to authorized individuals (US citizens or nationals) with the NTK.
- Ensure hardware is <u>not visible</u> from outside the space.

NNPI Storage

- Any time NNPI is not in the direct control of an authorized person, it should stored in a key lock container or lockable office or shop (locked area).
  - File cabinet, desk, safe
- Only authorized persons with a NTK may have access to the NNPI.
- "Container or locked area" should not have any external labels indicating the sensitivity of the contents.
- Material must not be visible from outside the "container or locked area".



NNPI Physical Storage Requirements

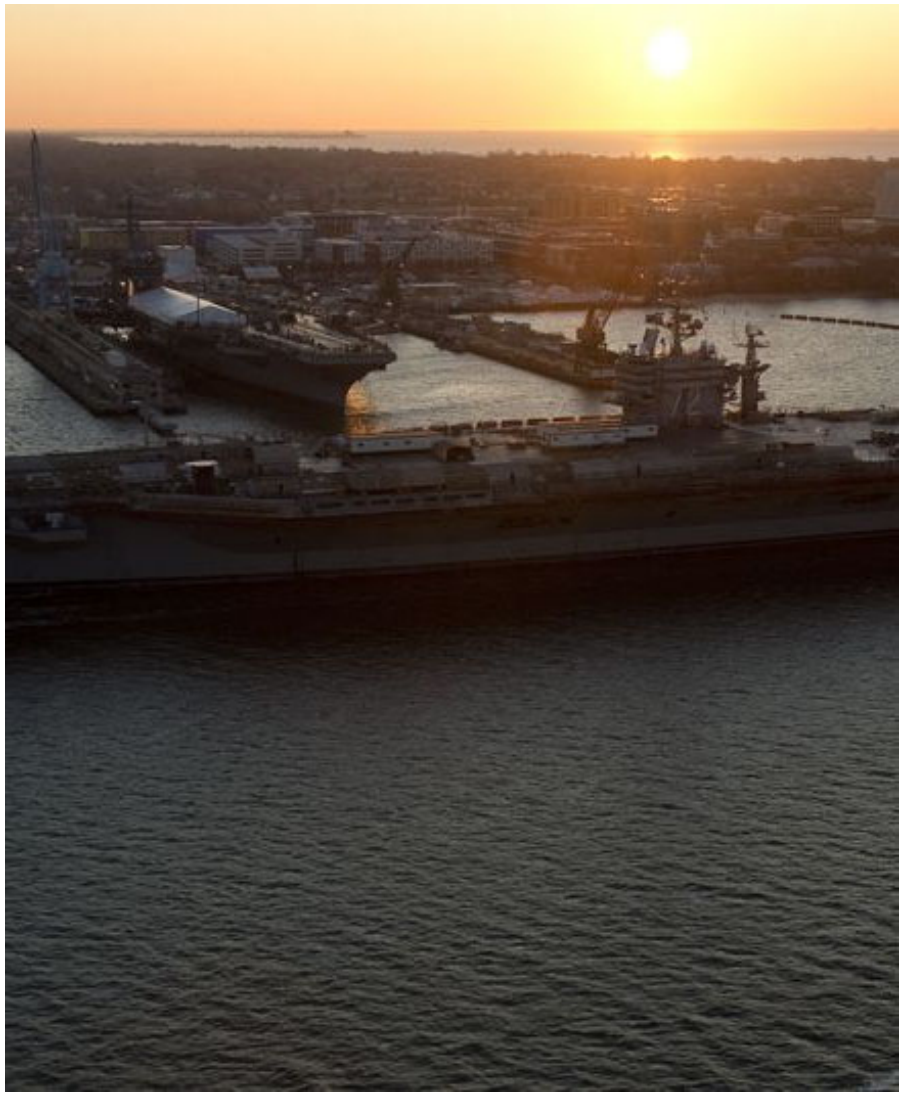
- All entry points to the "container or locked area" must be key-lockable. Crypto-locks are not adequate.
- Establish and document a strict key-control regimen to ensure only authorized individuals will access.
- The "container or locked area" must be constructed such that attempts at unauthorized entry are obvious.

NNPI Disposal & Destruction

- Unless NNS authorizes retention by the supplier, NNPI documents or media no longer required for contract execution shall be:
  - Securely returned to NNS; or
  - Destroyed using a shredder approved for classified destruction, per the NSA Evaluated Products List

Disclosure Policy for NNS Suppliers

- Supplier shall report to their NNS buyer any attempts by unauthorized persons to elicit NNPI
- Any known or suspected compromises of NNPI
  - Includes intentional or unintentional public release via such methods as:
    - Known or suspected compromise of the Supplier's information systems
    - Transmission via email
    - Placement on a web site
    - Improper disposal
    - Theft



Points of Contact

- NNS NNPI Control Officer
  - Stephen Simmons
  - Office: (757) 688-5287
  - Stephen.Simmons@hii-nns.com
- NNS Supplier Data team
  - SupplierData@hii-nns.com
- HII Exostar Team
  - Exostar@hii-nns.com
- HII External Supplier Website
  - https://supplier.huntingtoningalls.com