External Supplier Webinar: Sensitive Information, Cybersecurity and Data Protection

Newport News Shipbuilding
A Division of HII

Eva Latimer, Allyson Ladner, and Greg Bandish
Nov. 18th and Nov. 19th, 2025

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!

Presentation Speakers

Eva Latimer

Manager, Regulatory Compliance
Newport News Shipbuilding

Allyson Ladner

Cybersecurity Supply Chain Risk
HII

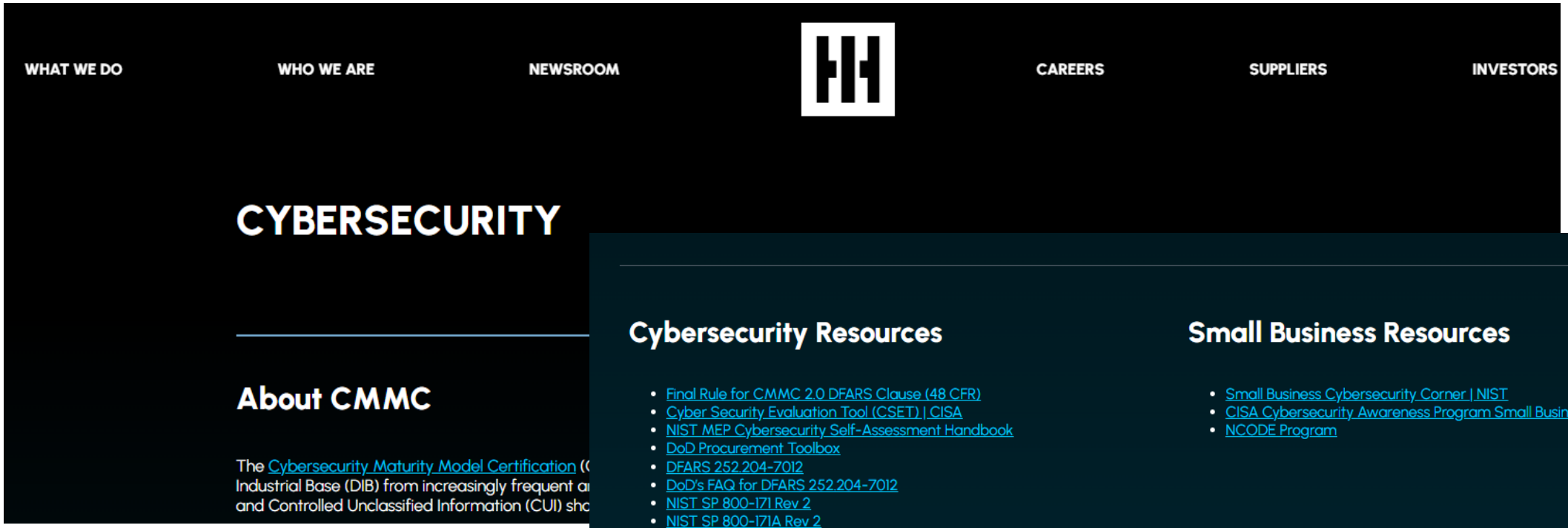
Greg Bandish

CMMC Program Manager
Oxford Global Resources

Agenda Topics

1. Supplier Support & Resources
2. Cybersecurity & BitSight
3. Federal Contract Information (FCI)
4. Controlled Unclassified Information (CUI)
5. CMMC Model 2.0 Requirements
6. Naval Nuclear Propulsion Information (NNPI)

Supplier Support & Resources
HII.com/Cyber



Cybersecurity Resources

- Final Rule for CMMC 2.0 DFARS Clause (48 CFR)
- Cyber Security Evaluation Tool (CSET) | CISA
- NIST MEP Cybersecurity Self-Assessment Handbook
- DoD Procurement Toolbox
- DFARS 252.204-7012
- DoD's FAQ for DFARS 252.204-7012
- NIST SP 800-171 Rev 2
- NIST SP 800-171A Rev 2
- NIST 800-53R4 Security and Privacy Controls for Federal Information Systems Rev 5
- CyberAssist – DIB SCC CyberAssist (ndisac.org)
- CMMC 2.0 Supplier Letter
- Chief Information Officer – U.S. Department of Defense
- DoD CUI Program > About CMMC
- DoD CUI Program > CMMC Resources and Documentation
- DoD CUI Program > CMMC FAQs
- DoD CUI Program > CUI Registry New
- Implementing the Cybersecurity Maturity Model Certification (CMMC) Program
- CMMC Accredited Body
- NSA Cybersecurity Collaboration Center
- HII CMMC Timeline
- CMMC Letter to Suppliers 9/11/2025

Small Business Resources

- Small Business Cybersecurity Corner | NIST
- CISA Cybersecurity Awareness Program Small Business Resources | CISA
- NCODE Program

BitSight

NNS uses a third-party service that helps HII assess and monitor the “external facing” cybersecurity posture of our Suppliers.

Supply Chain Management	Continuous Monitoring	Compliance and Reporting	Risk Mitigation	Competitive Advantage
• Identification of vulnerabilities • Provides security rating to support informed decisions	• As opposed to periodic assessments • Enables real-time awareness of potential security risks • Proactive response before vulnerability is exploited	• Ensures compliance with industry standards and regulations • Demonstrates active management of Supply Chain cybersecurity risks	• Identifies gaps • Allows action to mitigate risks • Potentially reduces cyberattack likelihood	• Differentiator when bidding for contracts • Demonstrates higher level of cybersecurity due diligence

BitSight and Supplier Actions

For BitSight access, send request to HIICyberSCM@hii.com

Working Together on Cybersecurity Posture

- Access to Suppliers no cost
- Supplier can be notified of vulnerabilities to take action to remediate
- HII Cybersecurity monitors critically identified vulnerabilities by Supplier
- Un-remediated critical vulnerabilities may result in a change to electronic delivery of sensitive information

Take immediate action on Critical vulnerabilities!

Protecting Sensitive Information

It is everyone’s responsibility to protect sensitive information. Three common forms of information distributed or received by NNS are:

- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Unclassified Naval Nuclear Propulsion Information (U-NNPI)

FCI and CUI

FCI

Information not intended for public release that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public or simple transactional information, such as necessary to process payments.

48 CFR 52.204-21

CUI

Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using **safeguarding or dissemination controls**.

32 CFR Part 2002

FCI and CUI are information that is ‘not intended for public release.’ However, CUI requires additional safeguarding and may also be subject to dissemination controls.

What are examples and what is required to receive the information?

Sensitive Information Requirements Matrix for Electronic Transmissions

The below matrix outlines requirements for sensitive information received by Suppliers from NNS. There are physical protection requirements to receive sensitive information in hard copy format.

Sensitive Information Category	Category or Document Marking Examples commonly seen from NNS include, but not limited to:	Examples include, but are not limited to:	Cybersecurity Evidence Controls	Electronic Transmission
FCI	No marking required	Any Request for Quote (RFQ) or Purchase Order (PO) that ties back to a Navy/DoD Contract, even	Self-attestation of 15 controls implemented from FAR 52.204-21	Upon self-attestation
	Examples (FOUO, OUO)	DoD-Commercial		
CUI not requiring a JCP	Legacy markings:	Appendix B-DoD	Submission of NIST SP 800-171 Questionnaire in Exostar's Supplier Management Or C3PAO Certificate Or SPRS evidence supporting Self-Attestation or Certification (PDF)	Conditional upon HII Cybersecurity evaluation of submitted evidence
	Distribution Statements B-F, without export controlled markings			
CUI requiring a JCP	Legacy markings:	Appendix K		
	Distribution Statements B-F, with export controlled markings			

Transmission of FCI and CUI - Hardcopy

Manages cybersecurity risk of our supply chain based on a three-pronged approach:

The hardcopy transmission methods are the same for FCI and 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 external markings that would indicate sensitivity of contents
- Hand delivered or viewed at NNS

If NNS sends sensitive information to your company via hard copy, do not upload this information to your networks or information systems.

Transmission of FCI and CUI - Electronic

The electronic transmission methods are the same for FCI and CUI.

- Exostar Forum Pass/Information Manager available until 12/31/25
- Virtru application – Coming soon
- Email Encryption employing FIPS 140-2/140-3 encryption solution
- Physically mailed to the recipient's address
- Fax machines, to include networked

FCI and CUI Controls

When In Use

Storage

Disposal and Destruction

Concepts outlined below may not be all inclusive, depending on sensitivity nature of material.

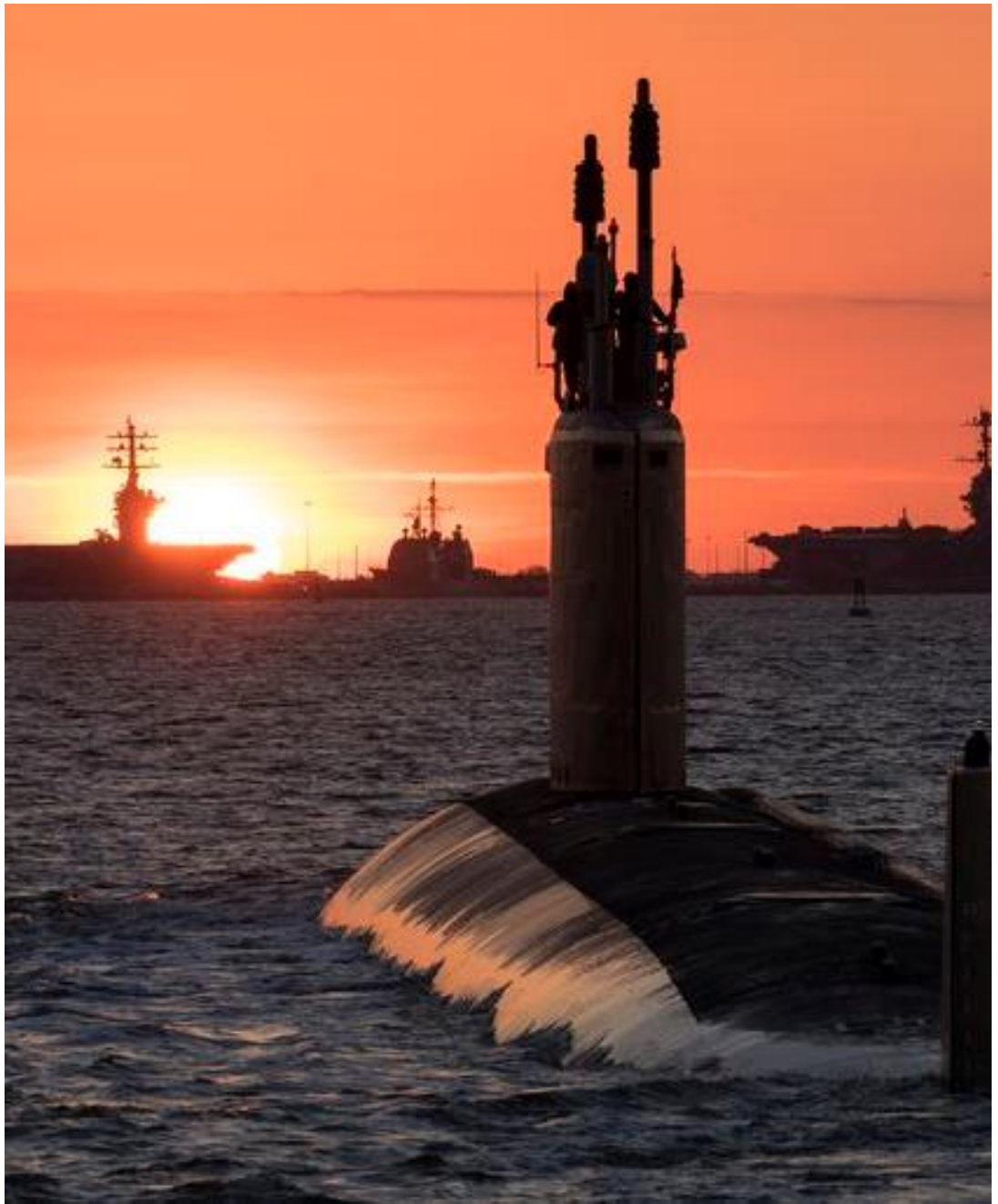
- Control information posted or processed on publicly accessible information systems.
- Controlled so that those without authorized access & a Need To Know (NTK) cannot obtain visual or physical access that would permit detailed examination.
- Prevent exposure of export-controlled and controlled technical information to foreign nationals.
- Materials should be put away, covered, or turned face-down anytime persons without NTK are present.

- Physical protection controls
  - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
  - Escort visitors and monitor visitor activity.
  - Maintain audit logs of physical access.
  - Control and manage physical access devices.
- 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
- Requires a sturdy container or designated room or closet that:
  - Is secured by a key-operated lock
  - Shows immediate signs of tampering to access

- Unless NNS authorizes retention by the Supplier, 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 or data

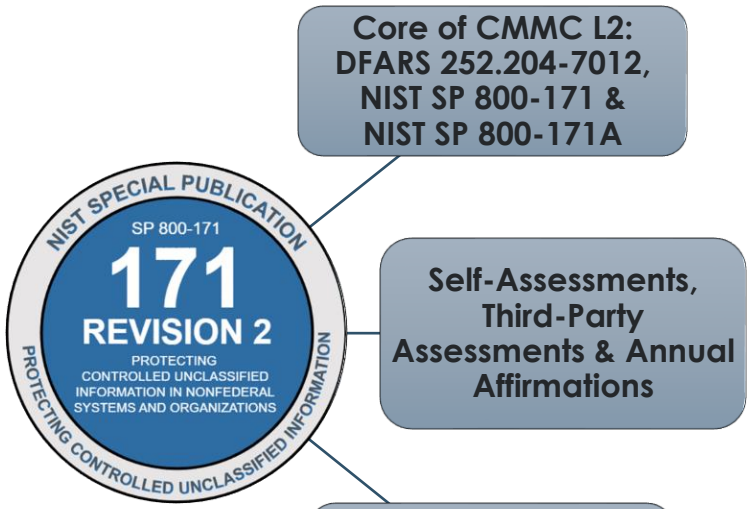
Supplier-Originated CUI Documents

Supplier-originated documents that reproduce, expand upon, or modify information drawn from documents that now contain CUI must have the appropriate marking.



What is CMMC?

Verifying that companies are actually implementing the cybersecurity practices they've committed to, ensuring proper protection of FCI and CUI across the DIB supply chain.



Core of CMMC L2: DFARS 252.204-7012, NIST SP 800-171 & NIST SP 800-171A

Self-Assessments, Third-Party Assessments & Annual Affirmations

Key Requirements: SSP & POA&M

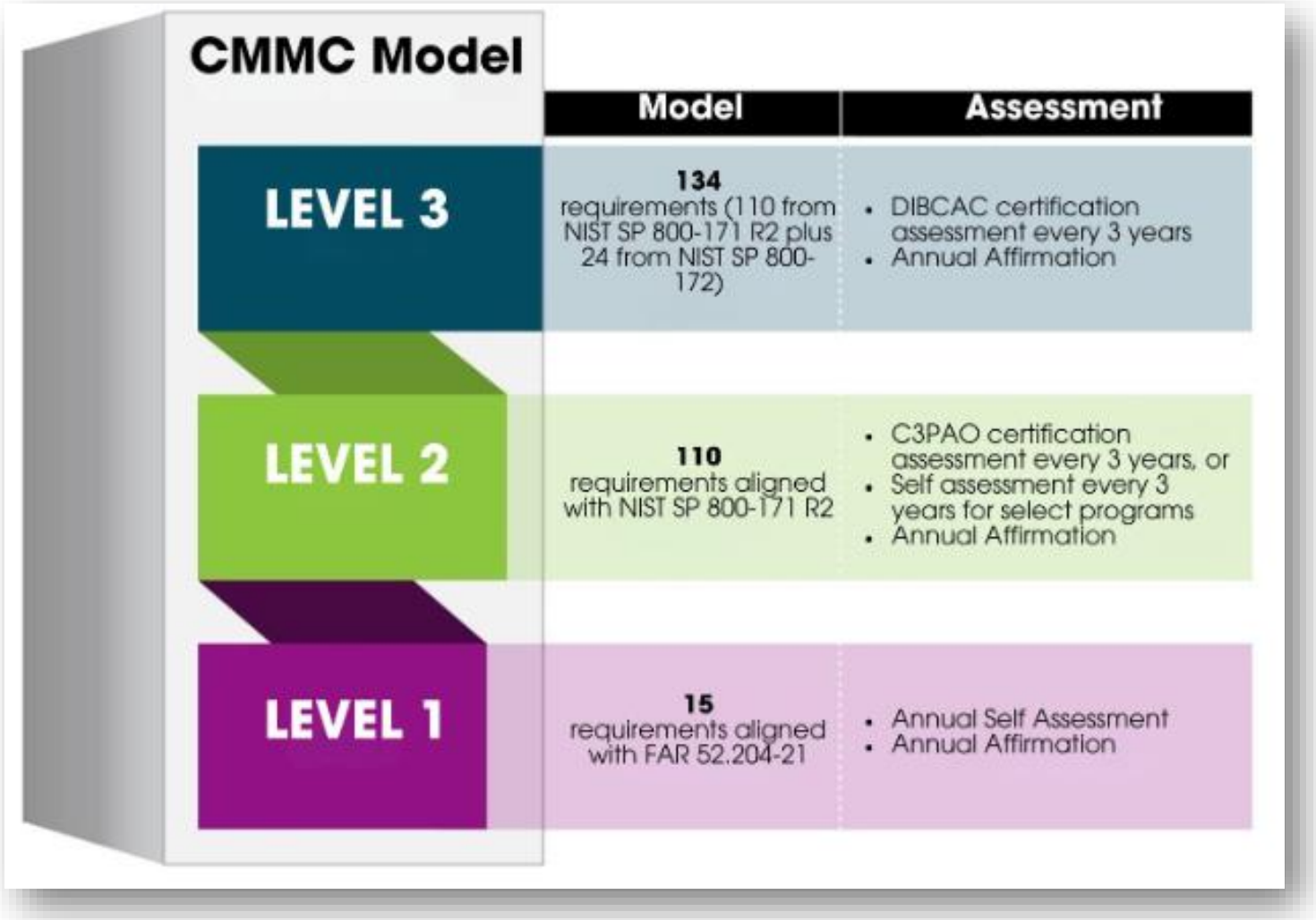
Level	Information Type	Method
Level 1	**FCI:** Information that is not intended for public release and is provided by or generated for the government under a contract to develop or deliver a product or service to the government.	Self-Assess
Level 2	CUI Categories **outside** the NARA CUI Registry **Defense** Organizational Index Grouping**:** *Critical infrastructure, Financial, Immigration, Intelligence, International, Agreements, Law Enforcement, Export Control (non-Defense), Legal, Natural and Cultural Resources, NATO, Nuclear, Patent, Privacy, Procurement & Acquisition, Proprietary Business Information, Statistical, Tax, and Transportation.*	Self-Assess (Unless PM deems high risk)
	CUI Categories **in** the NARA CUI Registry **Defense** Organizational Index Grouping**:** *Controlled Technical Information (CTI), DoD Critical Infrastructure Security Information (DCRIT), Naval Nuclear Propulsion Information (NNPI), Privileged Safety Information (PSI), and Unclassified Controlled Nuclear Information – Defense (DCNI).*	**Certification**
Level 3	• CUI associated with a breakthrough, unique, and/or advanced technology; • Significant aggregation or compilation of CUI in a single IS or IT environment; and • Ubiquity – when an attack on a single IS or IT environment would result in widespread vulnerability	Certification

CMMC Levels

Tiered Model: Security requirements scale with sensitivity of data

Assessments: Verifies compliance through independent review

Contracts: Certification required to win and hold work

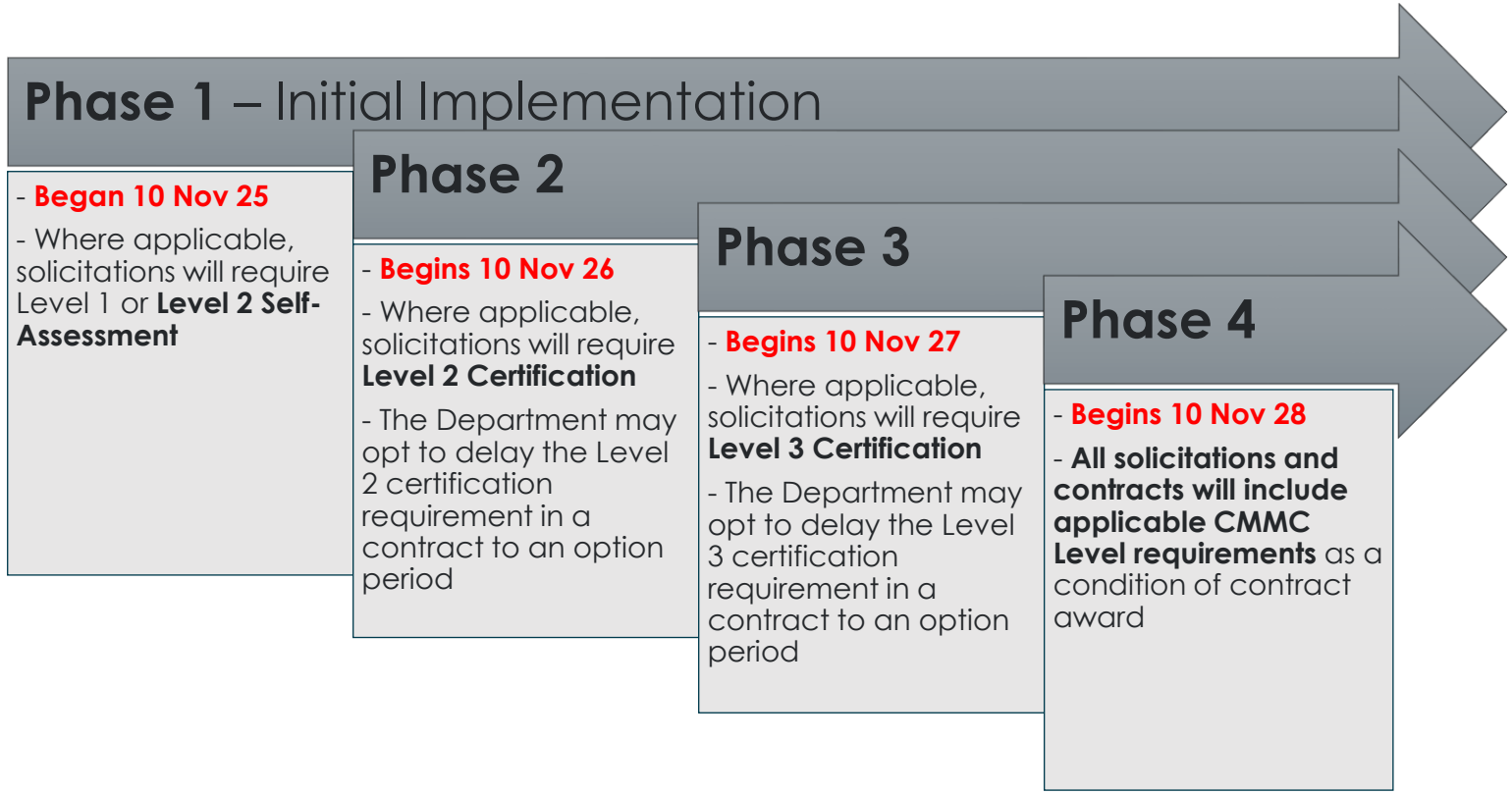


CMMC Phased Rollout

Start Date: November 10, 2025

Four-Phases: Implemented over 3 years, adding requirements in stages

Purpose: Allows time for assessor training and industry readiness



In some procurements, CMMC requirements may be implemented in advance of the planned phase.

CMMC Asset Categories

You need an **accurate inventory** of your assets before you can work on protecting it.

Asset categorization is the **foundation** of CMMC readiness

CUI Assets: Systems, devices, or tools that process, store, or transmit CUI. Think of them as the places where sensitive contract-related data lives. (*e.g., a virtual or physical workstation used by authorized personnel to access CUI related to a government contract*)

Security Protection Assets (SPAs): Systems or tools that protect CUI assets, like firewalls, antivirus software, or authentication systems. (*e.g., a firewall that prevents unauthorized access to a server holding CUI*)

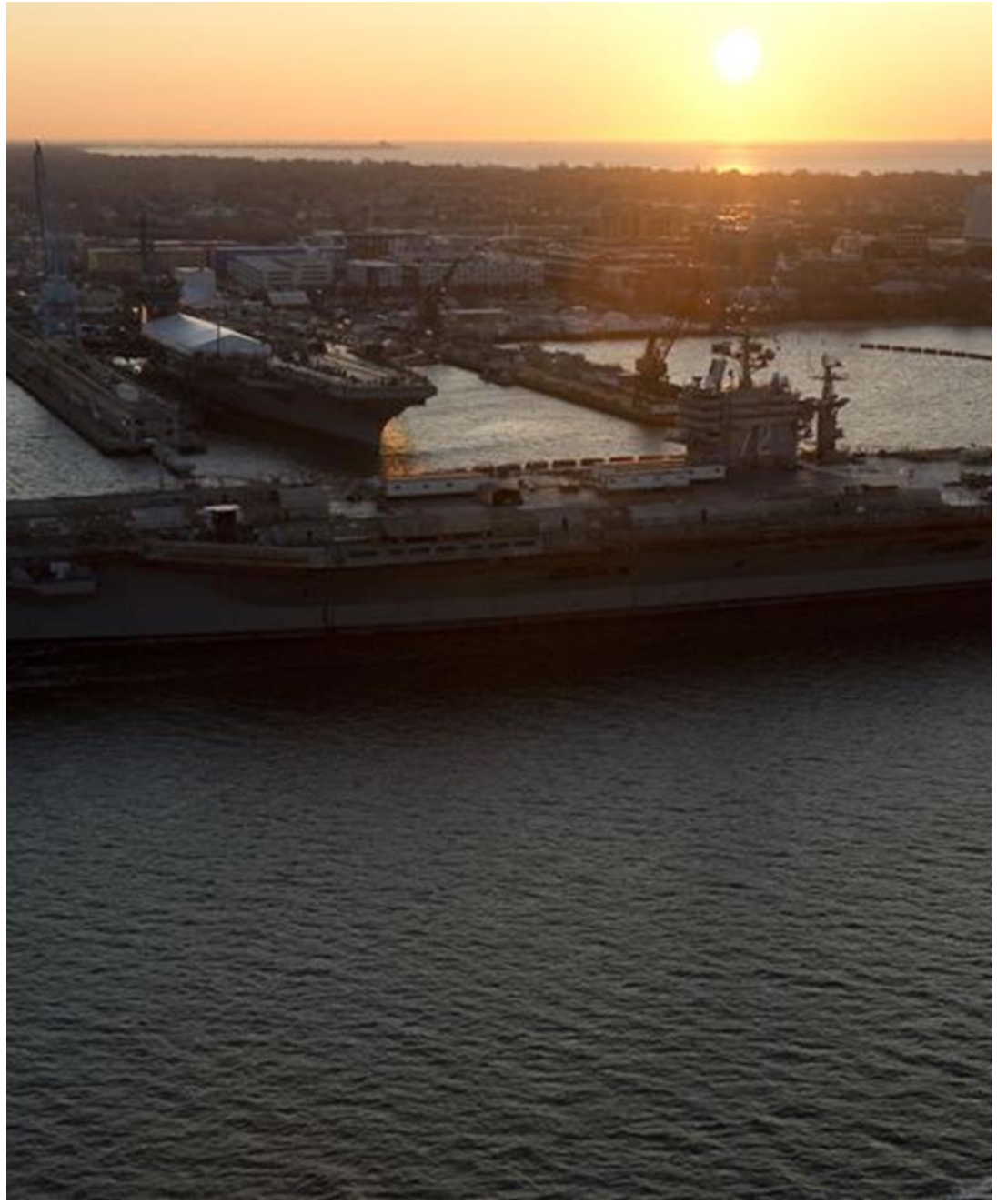
Contractor Risk Managed Assets (CRMAs): Company-owned systems that don't touch CUI directly but still connect to your network. You decide how to manage the risk they pose. (*e.g., a company-issued laptop used by a project manager to access internal business systems which is on the same enterprise network, but doesn't process, store, or transmit CUI*)

Specialized Assets: Non-traditional devices like smart sensors or industrial machines that are hard to secure using standard methods. (*e.g., a CNC machine connected to a network that can't run antivirus software*)

Out-of-Scope Assets: Assets that have no connection at all to CUI or the systems that protect it. They're completely outside of the CMMC boundary (*e.g., a visitor check-in kiosk located in the building lobby*)

eProcurement Tools

- NNS has two eProcurement tools for NNS and Suppliers to communicate.
  - Exostar Forum Pass / Information Manager active until 12/31/25.
  - Does not impact Exostar Supply Chain Platform (SCP)
  - **Virtru** – Coming Soon --- Allows sending of secure files to suppliers. Security features include watermarks and preventing of download of files based on Suppliers ability to receive documents. Also includes an expiration date whereby Supplier no longer has access.
    - Zero Cost to Suppliers
  - **Shipbuilding Partners and Suppliers (SPARS),** is a two way data exchange process to provide NNS suppliers with a means to transmit data pertaining to a Request for Quote (RFQ), Vendor Information Request and Purchase Order (PO) deliverable software that requires approval prior to authorizing manufacturing work release, hardware material shipment and post software submittal (i.e. vendor design drawings, sourcing bid information, technical manuals, welding and Non-destructive test procedures, etc.).
- Both SPARS and Virtru applications are **not authorized** for U-NNPI transmittals to or from NNS.
- Email EProcurementTools@hii-nns.com to report any instances where you receive U-NNPI from NNS via one of these tools.



Pre-submittal Requirements for Defense Logistics Agency (DLA) Joint Certification Program (JCP)

Active Commercial and Government Entity (CAGE) Code

Current System for Award Management (SAM) registration

Complete NIST SP 800-171 assessment and load scores into Supplier Performance Risk System (SPRS)

Complete DD Form 2345 (JCP application)

Use the NNS Supplier Compliance Card to determine the JCP expiration date and submit JCP Application **EARLY**

NNS Supplier Compliance

Supplier Compliance - NNS is taking a proactive approach to keeping the Supplier informed of 'key dates' to ensure the Supplier is aware of the expirations. Please reach out to contact our Supplier Notification shared inbox at NNSSupplierNotification@hii-nns.com related to any questions or concerns. For additional information, please view our External Supplier Website at https://Supplier.HuntingtonIngalls.com.

Newport News Supplier ID:

Status: Current | Expiring | Expired

Field	Value	Description
SDC Expiration Date	3/8/2024	Expiration date for the Suppliers Representations and Certifications (SBF P9152 or SBF P9152R). This annual requirement affirms the information disclosed is current, accurate and complete. Upon expiration; the Supplier Account will be blocked and no new Purchase Order action can be taken. If the date is 'yellow'; it is a reminder the expiration date is approaching and action is required. If you have not already received the renewal request from the Supplier Data team; email the Supplier Compliance team at SupplierData@hii-nns.com. Our office will review your request and return forms required for renewal.
UEI (SAM)		This is the authoritative identifier to do business with the federal government. It is generated at https://sam.gov.
NNPI	Yes	This designates whether your company has been approved to receive Naval Nuclear Propulsion information (NNPI) or Unclassified Technical Data (UTD).
JCP Certification Number		The JCP Certification Number is used to certify contractors for access to unclassified technical data disclosing critcal technology controlled in the U.S. The JCP certification is site specific.
JCP Registr Expiration	2/13/2025	The expiration date for JCP Registration. Our office recommends 90 days prior to expiration working proactively with the Defense Logistics Agency (DLA) to obtain a new JCP expiration date. Questions regarding the requirments for the JCP Certification can be directed to the DLA.
CUI Transmission Approval	Electronic CUI Acceptable	This displays the method of Controlled Unclassified Information (CUI) transmission to the supplier. If hardcopy CUI is displayed; contact our Exostar team at Exostar@hii-nns.com to discuss actions required to move to the Electronic CUI status.
Electronic CUI Exp Date	4/24/2026	This is the last date the Buyer may forward CUI to your company electronically. Please ensure the NIST score in Exostar has not expired and work toward implementation of the 110 controls.

U-NNPI

FCI

48 CFR 52.204-21

CUI

32 CFR Part 2002

U-NNPI

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

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

U-NNPI

What is OPNAV N9210.3?

OPNAVINST N9210.3

- Guidance document for NNPI protections
- 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.

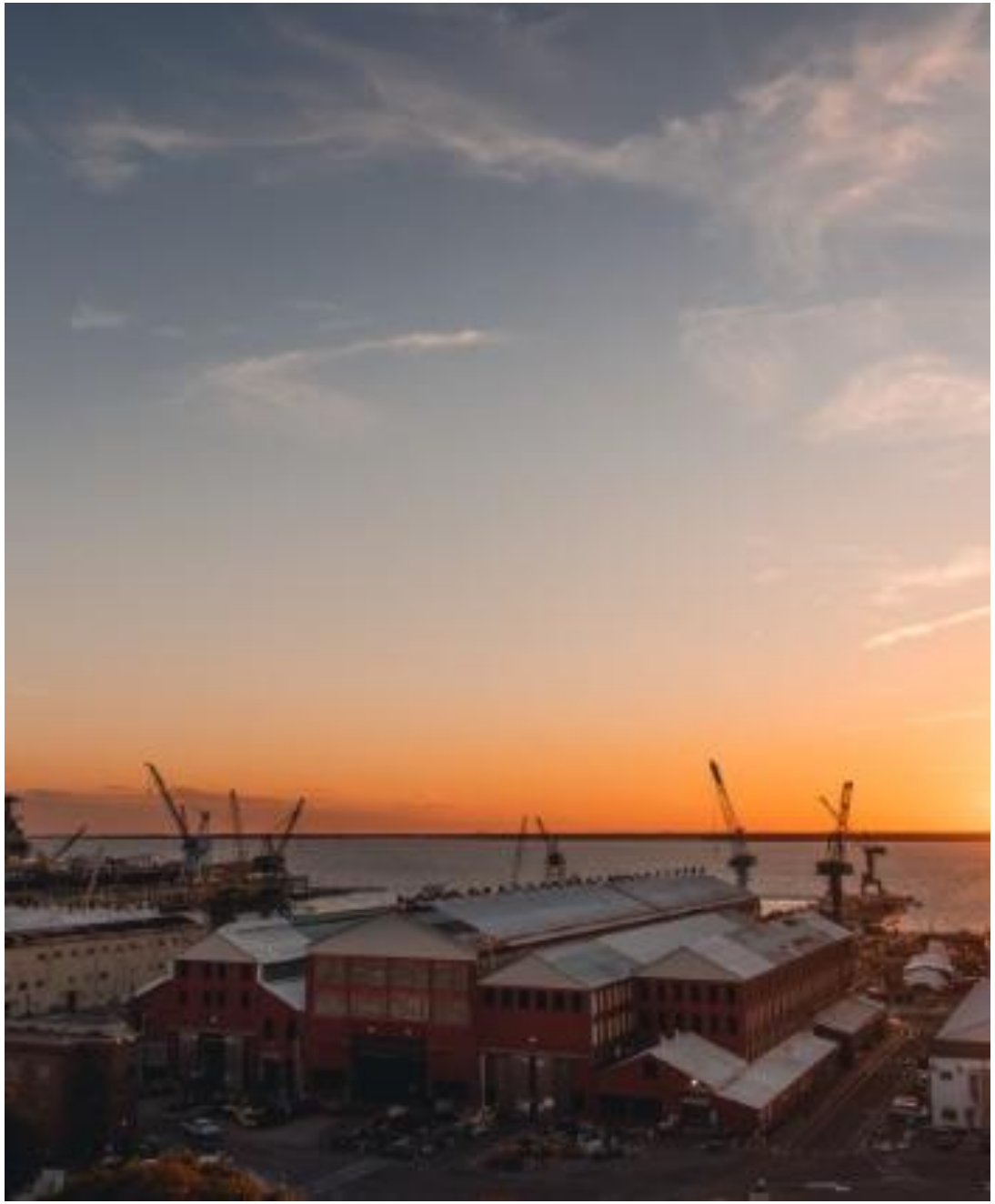
Sensitive Information Requirements Matrix for Electronic Transmissions

The below matrix outlines requirements for sensitive information received by Suppliers from NNS. There are requirements to receive U-NNPI in hard copy format, as outlined below.

Sensitive Information Category	Category or Document Marking Examples commonly seen from NNS include, but are not limited to:	Examples include, but are not limited to:	Cybersecurity Evidence Controls	Electronic Transmission
FCI	No marking required Examples (FOUO, OUO)	Any Request for Quote (RFQ) or Purchase Order (PO) that ties back to a Navy/DoD Contract, even DoD-Commercial	Self-attestation of 15 controls implemented from FAR 52.204-21	Upon self-attestation
CUI not requiring a JCP	Legacy markings: Distribution Statements B-F, without export controlled markings	Appendix B-DoD	Submission of NIST SP 800-171 Questionnaire in Exostar's OBM application	Conditional upon HII Cybersecurity evaluation of submitted NIST SP 800-171
CUI requiring a JCP	Legacy markings: Distribution Statements B-F, with export controlled markings	Appendix K		
U-NNPI (a subset of CUI that requires a JCP and completion of Form NN9540)	**NOFORN**	Unclassified Naval Nuclear Propulsion Information		Conditional upon HII Cybersecurity evaluation of submitted NIST SP 800-171 **and** receipt of NAVSEA08 ATO letter and **requires S/MIME encryption!**

Hardcopy Transmission of NNPI

- Faxed to a stand-alone fax machine
  - 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
- Physically Mailed
  - NNPI may be shipped within the US and its territories via Certified Mail or via express carrier (FedEx, etc.)
  - 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.
- Hand-delivered or viewed at NNS



U-NNPI Authorized Computers and Electronic Transmission

- U-NNPI may not be processed or stored on a Supplier-owned computer system or portable electronic device unless authorized by NAVSEA 08 Cybersecurity. U-NNPI may only be transmitted via the Internet to NAVSEA-approved computer systems.
  - S/MIME encryption is required
  - Ensure NNS Supplier Compliance team has the **NAVSEA 08 "Authorization to Operate" (ATO) in order to receive 'electronic' transmission of U-NNPI**
- Any removable media (thumb drives, CDs/DVDs, etc.) or external drives containing U-NNPI must be encrypted to FIPS 140-2 or 140-3 standards and must bear markings similar to those required for printed documents containing the same information.

U-NNPI Controls

When In Use

Storage

Disposal and Destruction

"Authorized individuals" are U.S. citizens or U.S. nationals with a Need to Know (NTK). Resident aliens ("green card" holders) are **prohibited**. NAVSEA 08 Security must be notified **before** granting access to Dual Citizens with NTK.

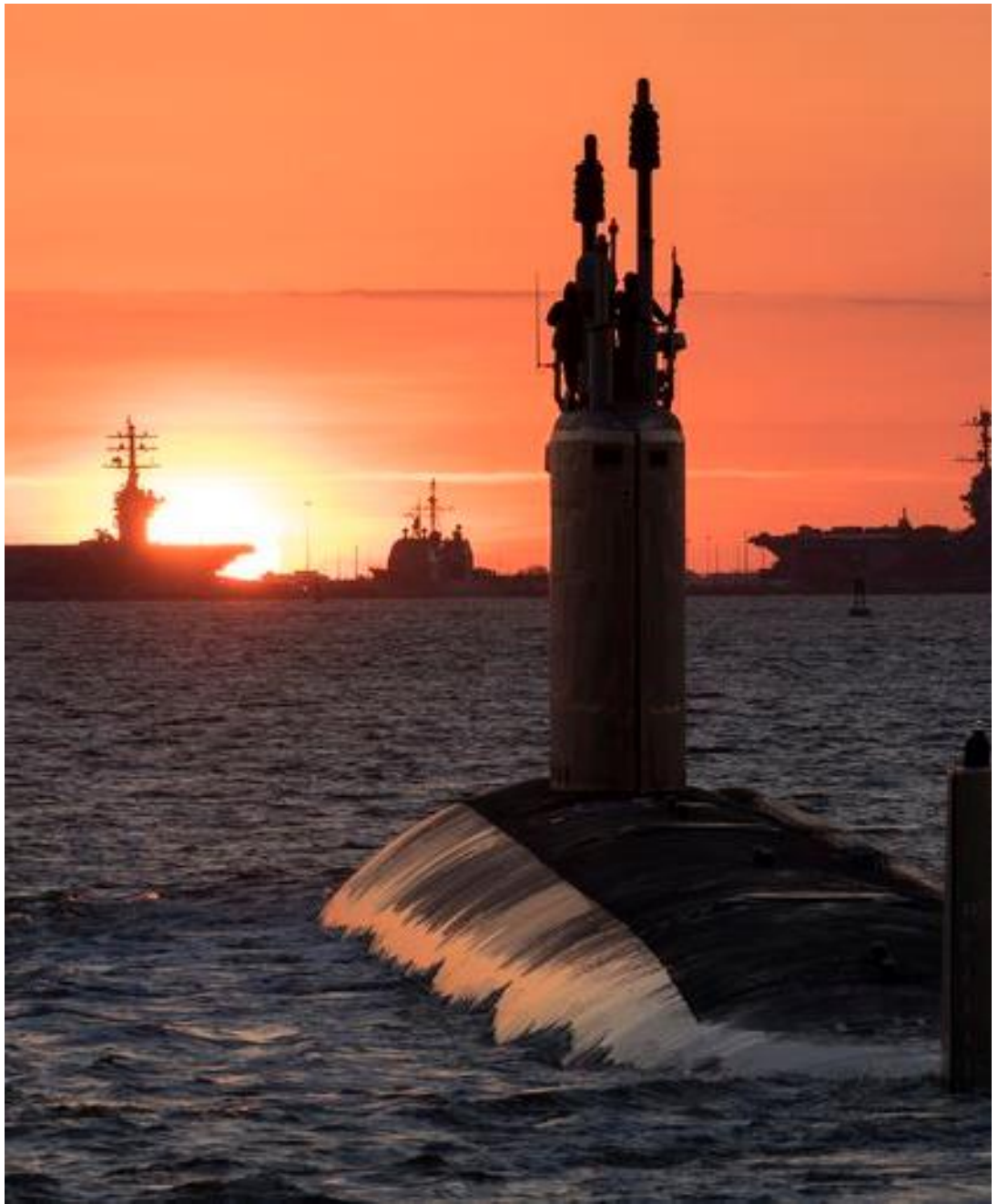
- Materials must remain under direct physical control by an authorized individual with NTK and in their personal possession.
- Must never be left unsecured, sent with checked baggage or left unattended in a vehicle
- Access to the space(s) where hardware is produced must be restricted to authorized individuals with NTK
- Not visible from outside the production area

- Access to the documentation or hardware is limited to those authorized individuals with a NTK
- Designed so documents and/or hardware are **not visible** from outside "container or locked area"
- A key-lockable "container or locked area"
  - File cabinet, desk or safe
  - Office or shop
  - Storage space
- "Container or locked area" must be constructed such that attempts at unauthorized entry are obvious
- Crypto-locks are not adequate
- "Container or locked area" should not have any external labels indicating sensitivity of contents
- Establish and document a strict key control regimen to ensure only authorized individuals with NTK will access.

- 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 found at https://nsa.gov/portals/75/documents/resources/everyone/media-destruction/epl-18-may-2015.pdf

Supplier-Originated U-NNPI Documents

- Supplier-originated documents that reproduce, expand upon, or modify information drawn from U-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.



U-NNPI Disclosure Policy for NNS Suppliers

- Supplier shall report to their NNS Buyer any attempts by unauthorized persons to elicit U-NNPI and any known or suspected compromises of U-NNPI
- Includes intentional or unintentional public release via such methods as:
  - Known or suspected compromise of the Supplier's information systems
  - Transmission via email or receipt of a CD requiring computer to open, without having a NAVSEA 08 ATO
  - Placement on a web site
  - Improper disposal
  - Theft

Questions -

Add any questions to the Chatbox.

Thank you for attending today's webinar.

Stay tuned --- A PDF copy of the webinar will be posted to the NNS Supplier website.