

External Supplier Webinar: Sensitive Information, Cybersecurity and Data Protection

Newport News Shipbuilding
A Division of HII

Greg Bandish, Jessica Borst, and
Troy Vuyovich
November 12-13, 2024



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

Jessica Borst



Sr. Regulatory Compliance Analyst
Newport News Shipbuilding

Troy Vuyovich

Certified Information Security Manager (CISM)



Cybersecurity Supply Chain Risk Manager
Huntington Ingalls Industries

Greg Bandish



CMMC Program Manager
Oxford Global Resources

Agenda Topics

- **Supplier Support & Resources**
- **Cybersecurity & BitSight**
- **Federal Contract Information (FCI)**
- **Controlled Unclassified Information (CUI)**
- **CMMC Model 2.0 Requirements**
- **Naval Nuclear Propulsion Information (NNPI)**



Supplier Support & Resources

HII.com/Cyber

WHAT WE DO

WHO WE ARE

NEWSROOM



CAREERS

SUPPLIERS

INVESTORS


CYBERSECURITY

About CMMC

The [Cybersecurity Maturity Model Certification \(CMMC\) 2.0](#) is an Industrial Base (DIB) from increasingly frequent and complex cyberattacks and Controlled Unclassified Information (CUI) shared within the

Cyber Incident Reporting

When a cyber-incident is discovered, contractors, subcontractors and suppliers must conduct a review for evidence of compromise of covered defense information and report to the DoD and HII within 72 hours. A "Cyber incident" is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

 [Report Cyber Incident to DoD](#)

Supplier Flow Down

When engaging with other suppliers that require access to covered defense information in performance of a contract, include the DFARS 252.204-7012 clause in any subcontracts, or similar contractual instruments with those suppliers. [Read the full clause here.](#)

Cybersecurity Resources

- [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](#)

Small Business Resources

- [Small Business Cybersecurity Corner | NIST](#)
- [CISA Cybersecurity Awareness Program Small Business Resources | CISA](#)



Supplier Support & Resources

Supplier Compliance Index Card

Supplier Compliance Index Cards are used to view important supplier information and upcoming expiration dates. These Index cards are distributed monthly.

Supplier Compliance Index Cards currently highlight Suppliers' CUI and if applicable, NNPI Transmission methods.



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 critical 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 requirements 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.

Future additions will include FCI Transmission Approval and Electronic FCI Exp. Date.



BitSight

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

Supply Chain Management

- Identification of vulnerabilities
- Provides security rating to support informed decisions

Continuous Monitoring

- As opposed to periodic assessments
- Enables real-time awareness of potential security risks
- Proactive response before vulnerability is exploited

Compliance and Reporting

- Ensures compliance with industry standards and regulations
- Demonstrates active management of Supply Chain cybersecurity risks

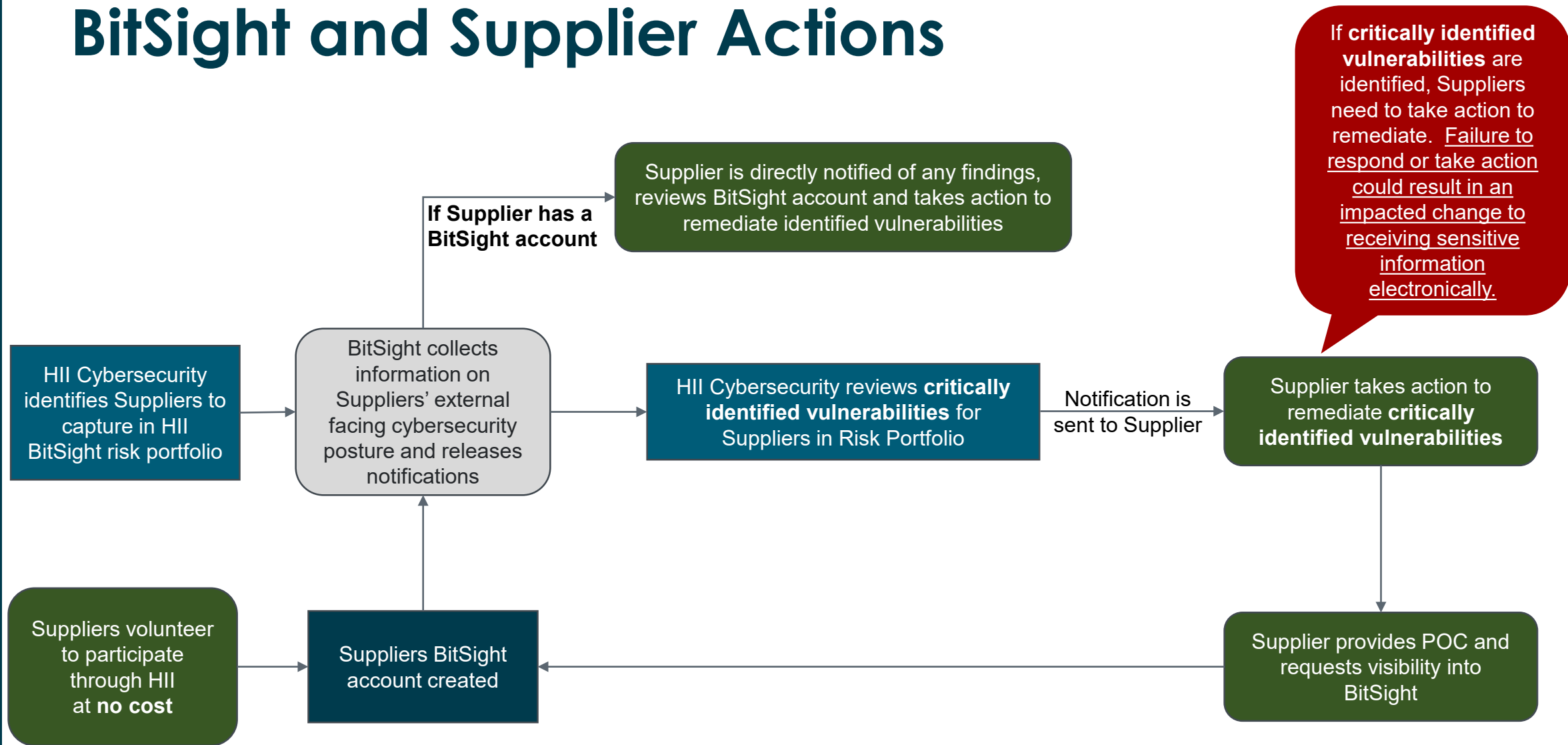
Risk Mitigation

- Identifies gaps
- Allows action to mitigate risks
- Potentially reduces cyberattack likelihood

Competitive Advantage

- Differentiator when bidding for contracts
- Demonstrates higher level of cybersecurity due diligence

BitSight and Supplier Actions

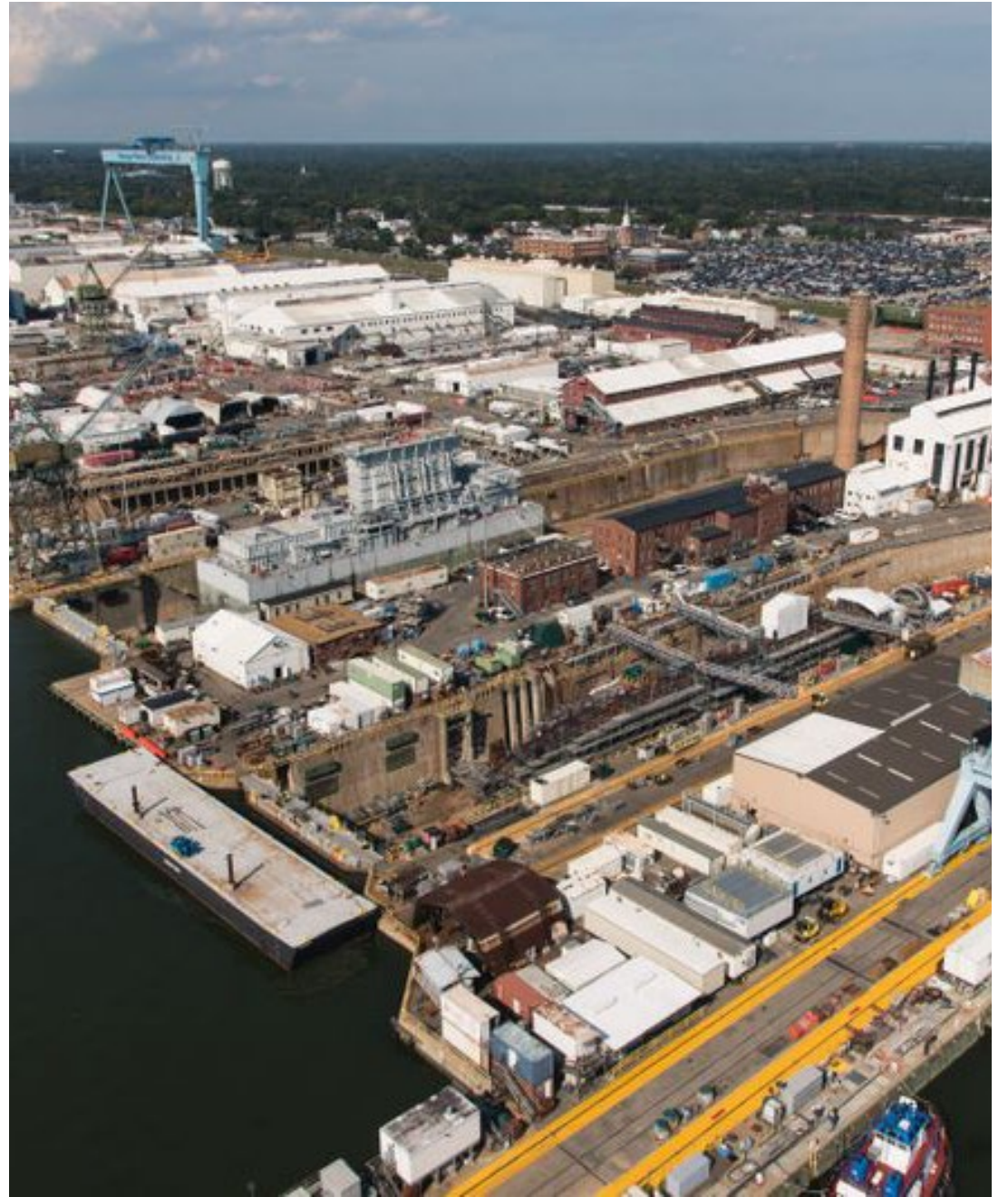


If critically identified vulnerabilities are identified, Suppliers need to take action to remediate. Failure to respond or take action could result in an impacted change to receiving sensitive information electronically.

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

All CUI in possession of a government contractor or subcontractor is FCI, but not all FCI is CUI.

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 currently no requirements to receive sensitive information in hard copy format.

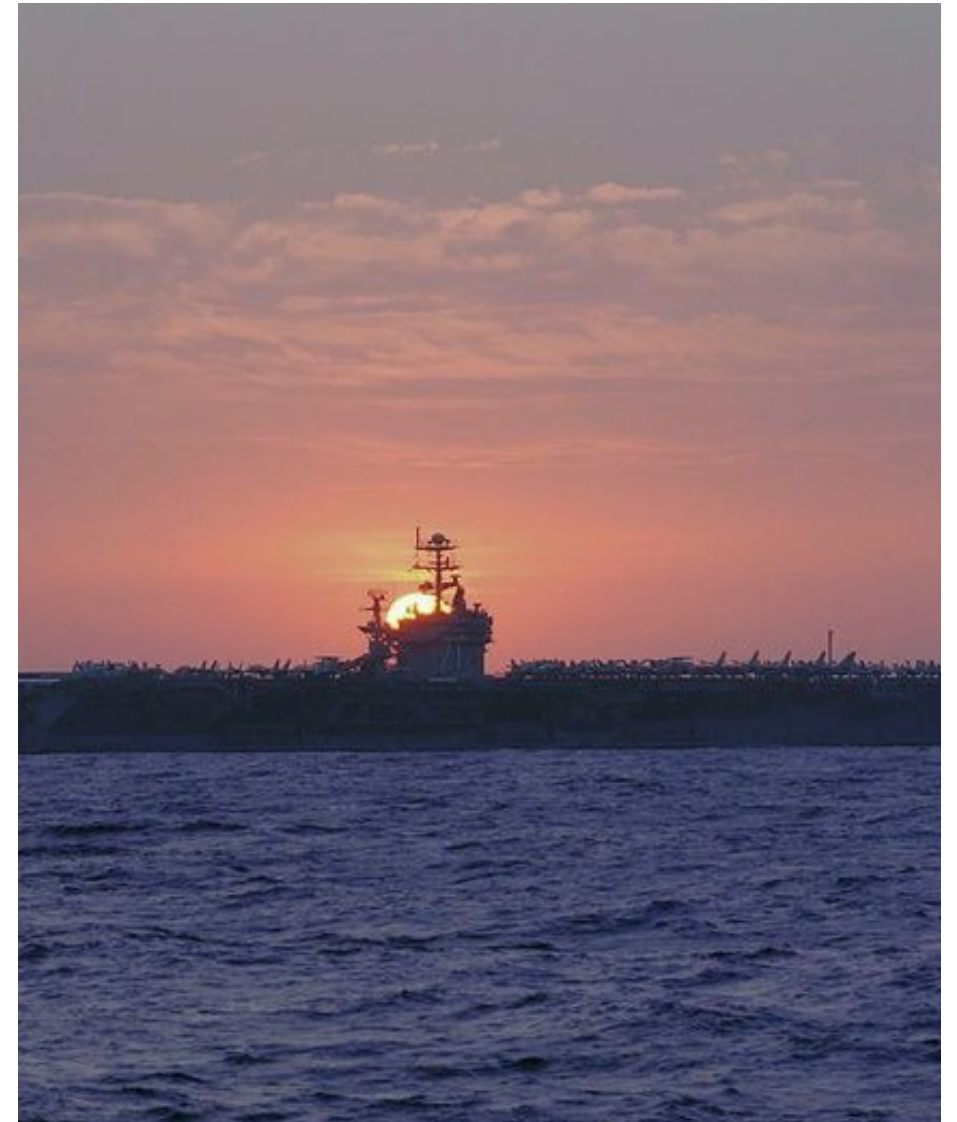
Sensitive Information Category	Category or Document Marking Examples commonly seen from NNS include, but are not limited to:	Examples include, but are not limited to:	Cybersecurity Evidence Controls	Electronic Transmission
FCI	No marking required	Any Request for Quote (RFQ) or Purchase Order (PO) that 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: FOUO, OUO, SBU, 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		



Transmission of FCI and CUI - Hardcopy

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

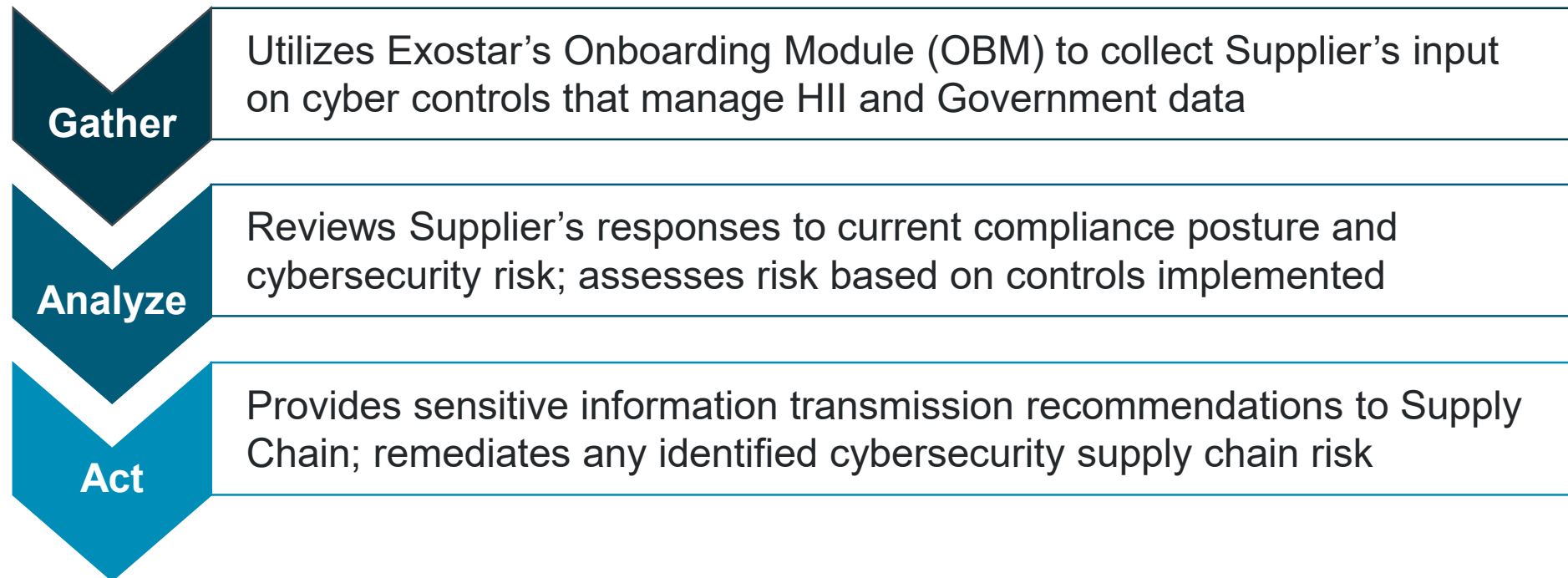
- May be sent to stand-alone fax machines
 - Faxed within the US and its territories provided there is an authorized person waiting to receive the document and properly control it; **AND**
 - Provided the receiving device is not connected to a computer
- Physically mailed after confirming recipient's 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 you via hard copy, do not upload this information to your networks or information systems.

HII's Supply Chain Cybersecurity Compliance Risk Mitigation Program (SC3RMP)

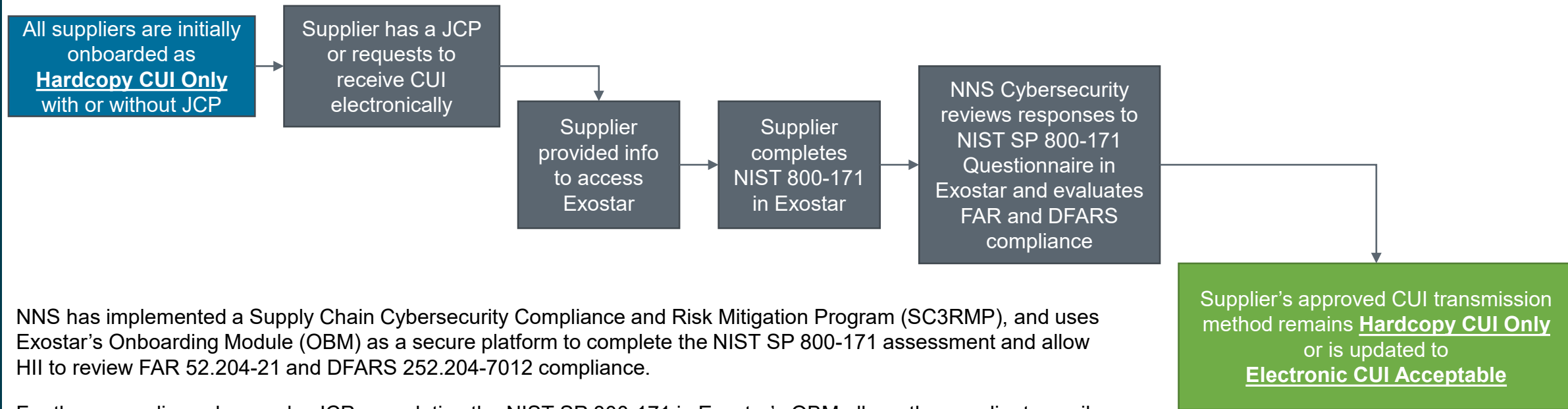
HII's SC3RMP manages cybersecurity risk of our supply chain based on a three-pronged approach:



HII Cybersecurity addresses compliance with applicable regulatory requirements, HII policies and contractual obligations.



Supplier Process for Evaluation to Receive Electronic CUI Transmissions



NNS has implemented a Supply Chain Cybersecurity Compliance and Risk Mitigation Program (SC3RMP), and uses Exostar's Onboarding Module (OBM) as a secure platform to complete the NIST SP 800-171 assessment and allow HII to review FAR 52.204-21 and DFARS 252.204-7012 compliance.

For those suppliers who need a JCP, completing the NIST SP 800-171 in Exostar's OBM allows the supplier to easily share their cyber security information 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 OBM application to complete the questionnaire.

Note: A self-attestation form is not required to be approved for electronic FCI transmission, if the NIST SP 800-171 Questionnaire is completed in Exostar's OBM application.



Electronic Transmission of FCI and CUI



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

- Exostar Information Manager application
- 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.

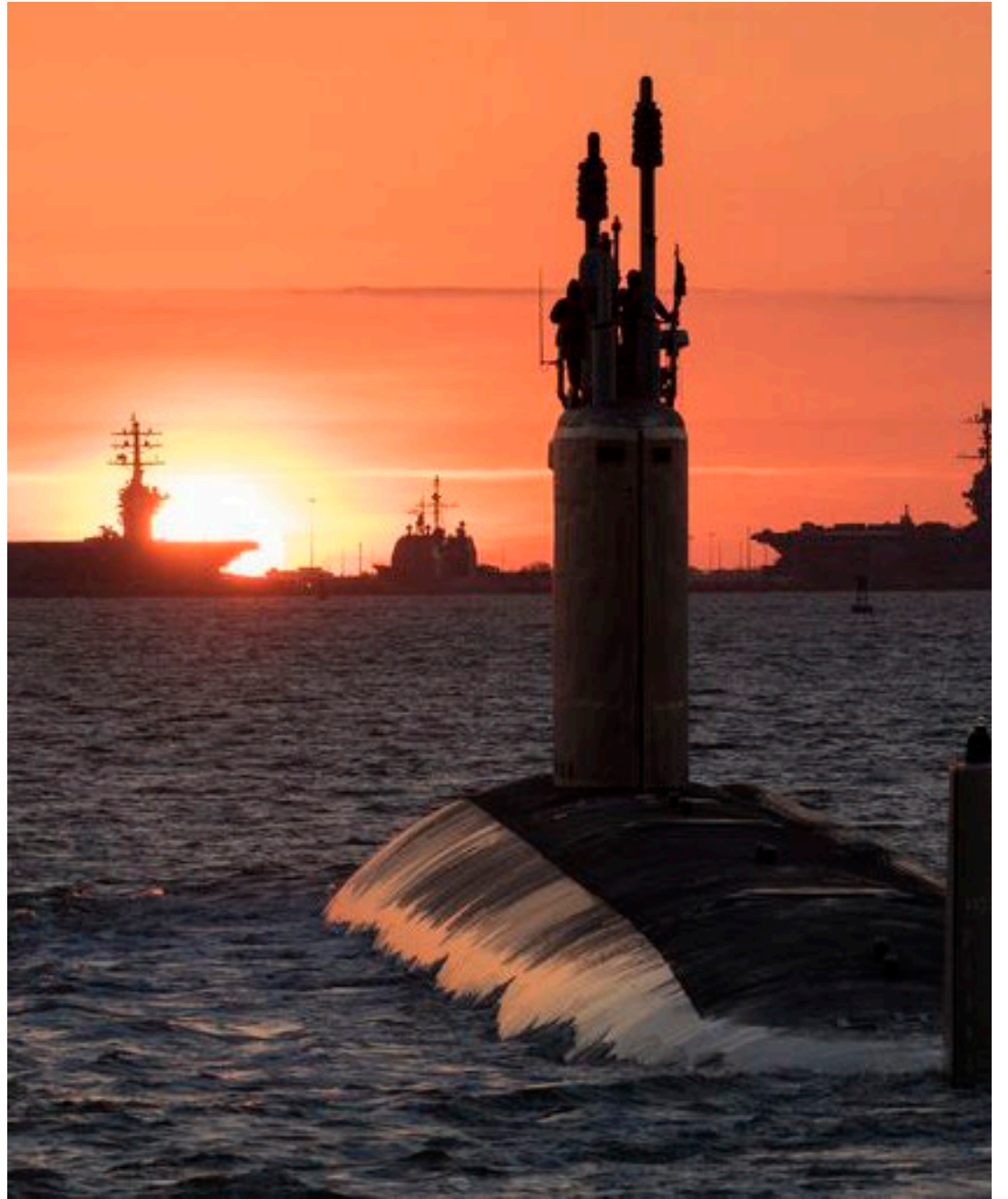
- Control information posted or processed on publicly accessible information systems.
- Controlled so that those without authorized access & a Need To Know (NTK) cannot obtain visual or physical access that would permit detailed examination.
- Prevent exposure of export-controlled and controlled technical 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.



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)

Submit JCP Application to DLA

[JCP Home \(dla.mil\)](https://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.



- Questions -

Please add any questions in the chat box.



CMMC Model 2.0

CMMC Model	Model	Assessment
LEVEL 3	134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	<ul style="list-style-type: none">• DIBCAC assessment every 3 years• Annual Affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171 r2	<ul style="list-style-type: none">• C3PAO assessment every 3 years, or• Self-assessment every 3 years for select programs.• Annual Affirmation
LEVEL 1	15 requirements aligned with FAR 52.204-21	<ul style="list-style-type: none">• Annual self-assessment• Annual Affirmation

Reference: <https://dodcio.defense.gov/CMMC/about>



Cybersecurity Compliance

DFARS 7012 Required Today

DFARS 7012 requires contractors to comply with **NIST SP 800-171** controls to protect **Controlled Unclassified Information (CUI)**.

A foundational part of defense contracting to ensure compliance with cybersecurity standards.

Responsible for SPRS Score

Today, contractors must submit their **SPRS score**, based on their NIST SP 800-171 self-assessment.

Upcoming CMMC requirements will require senior officials to submit **annual affirmations** to confirm ongoing compliance.

CMMC Re-Introduced As Model 2.0

A DoD program to increase assurance the **Defense Industry Base (DIB)** meets requirements to protect **CUI**.

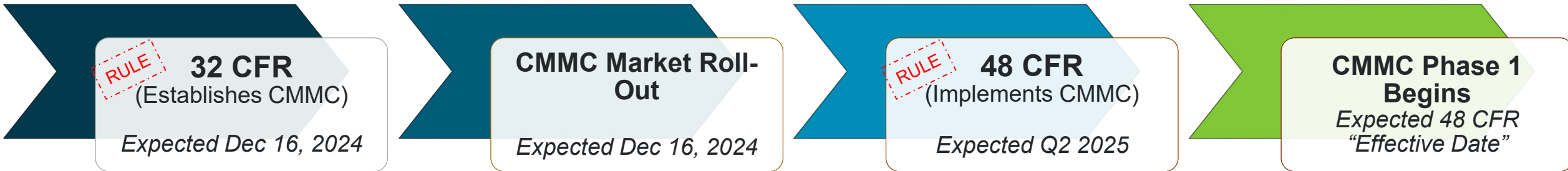
Estimated to take **12-18 months** for a DIB supplier to get **Level 2 certified**, for those required.

Evidence for Certification

Contractors must provide documented evidence such as **System Security Plans (SSPs)** and Data Flow Diagrams.

Artifacts are required to prove control implementation during assessments.

Anticipated Timeline



CMMC Phased Implementation

Phase 1: Self-Assessments

Begins at 48 CFR Rule Effective Date & requires self-attestation for Levels 1 and 2 on new contracts

Phase 2: CMMC Level 2 Certifications

12 months after Phase 1 start & requires C3PAO certification for Level 2 on new contracts

Phase 3: CMMC Level 3 Certifications

24 months after Phase 1 start & requires DIBCAC certification for Level 3 on new contracts and C3PAO certification for Level 2 on option exercises

Phase 4: Full Roll-out to All

36 months after Phase 1 start & all solicitations & contracts will include applicable CMMC Level requirements as a condition of contract award

Changes and Impact to Suppliers

Non-compliance risks losing new contract opportunities			
	Covered contractor information systems with FCI	Covered contractor information systems with CUI	Ongoing Responsibility
Current State	FAR 52.204-21 requires no self-attestation	DFARS 252.204-7012 relied on self-attestation for required compliance with NIST SP 800-171 (Rev 2)	Maintain SPRS scores in accordance with DFARS 252.204-7019
Future State, CMMC 2.0 introduces tiers	Level 1 compliance; will require annual self-attestation	Level 2 certification; will require 3rd party assessment	Maintain compliance for Level 1; maintain certification for Level 2

While CMMC builds on DFARs, it significantly increases **enforcement** and **accountability**.

Note: This slide is intended as a snapshot overview of requirements does not negate compliance with any additional requirements outlined by the regulations. Suppliers must follow the required security controls based on their level, ensuring FCI and/or CUI protection.

- Questions -

Please add any questions in the chat box.



U-NNPI

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.

**What is OPNAV
N9210.3?**

CUI

32 CFR Part 2002

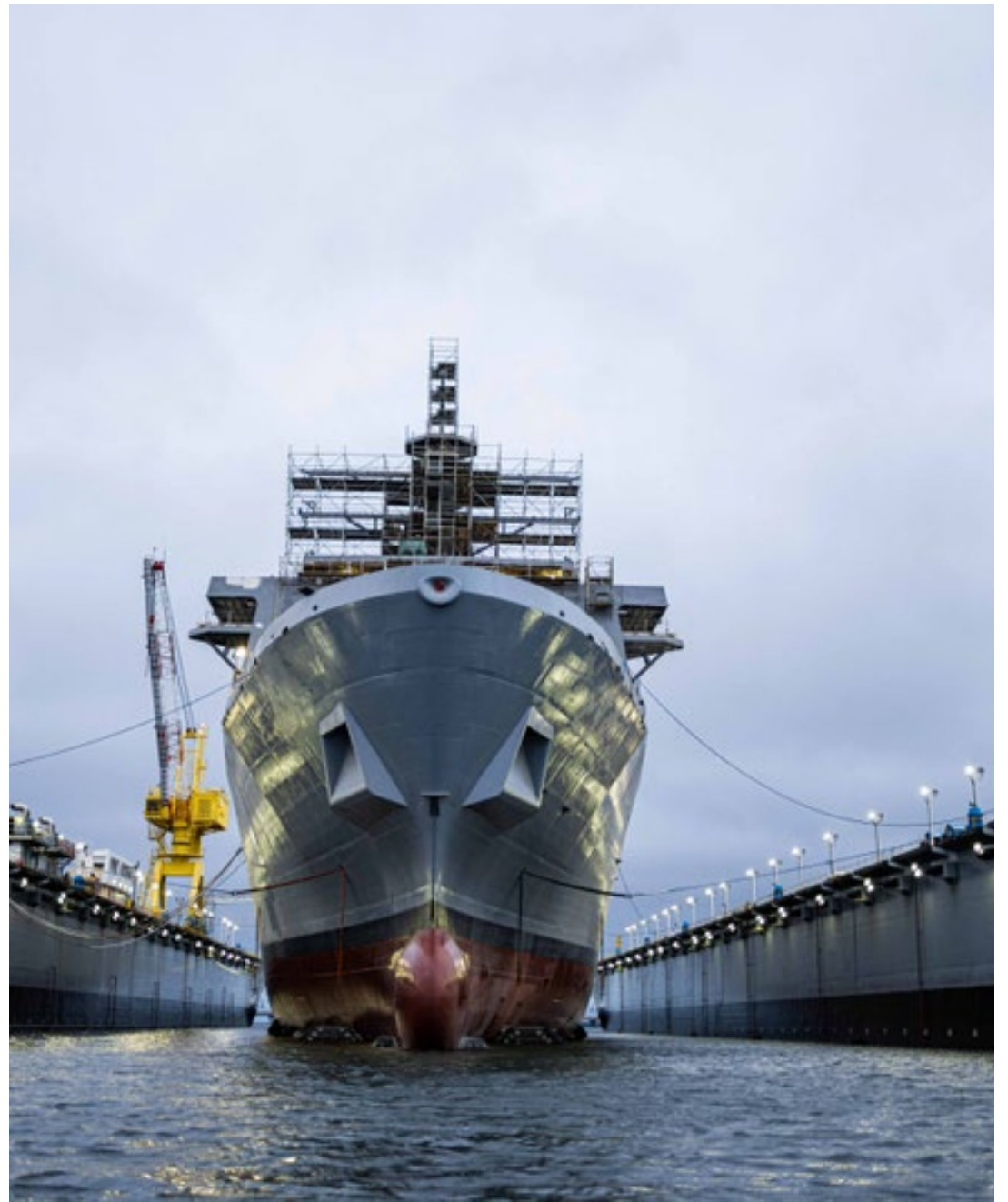
FCI

48 CFR 52.204-21

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

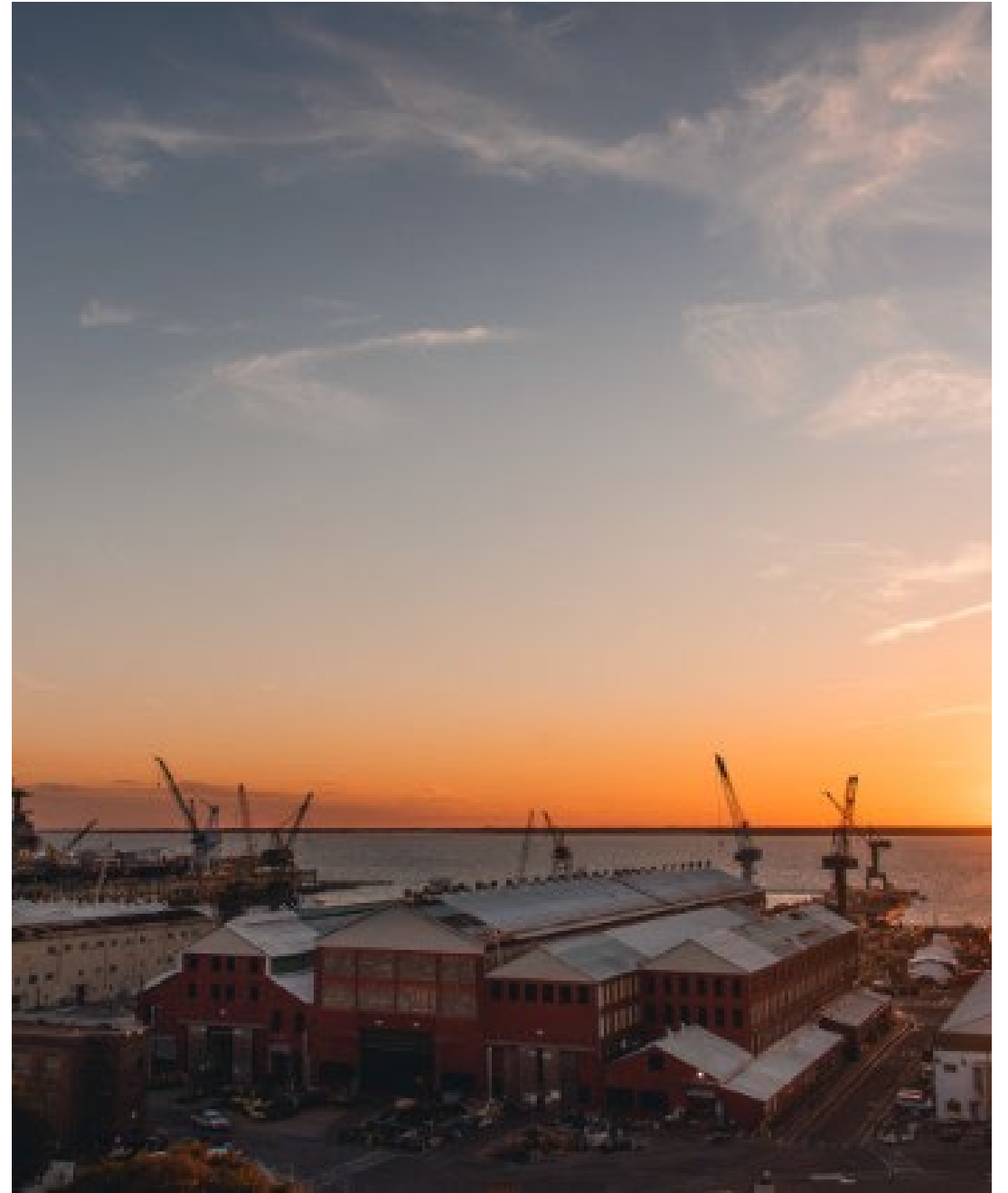
The below matrix outlines requirements for sensitive information received by Suppliers from NNS. There are currently no requirements to receive FCI and CUI in hard copy format, however, there are requirements to receive U-NNPI in hard copy format, as outlined below.

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	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: FOUO, OOU, SBU, 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 <u>and</u> completion of Form NN9540)	NOFORN	Unclassified Naval Nuclear Propulsion Information		Conditional upon HII Cybersecurity evaluation of submitted NIST SP 800-171 <u>and</u> 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.
 - 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



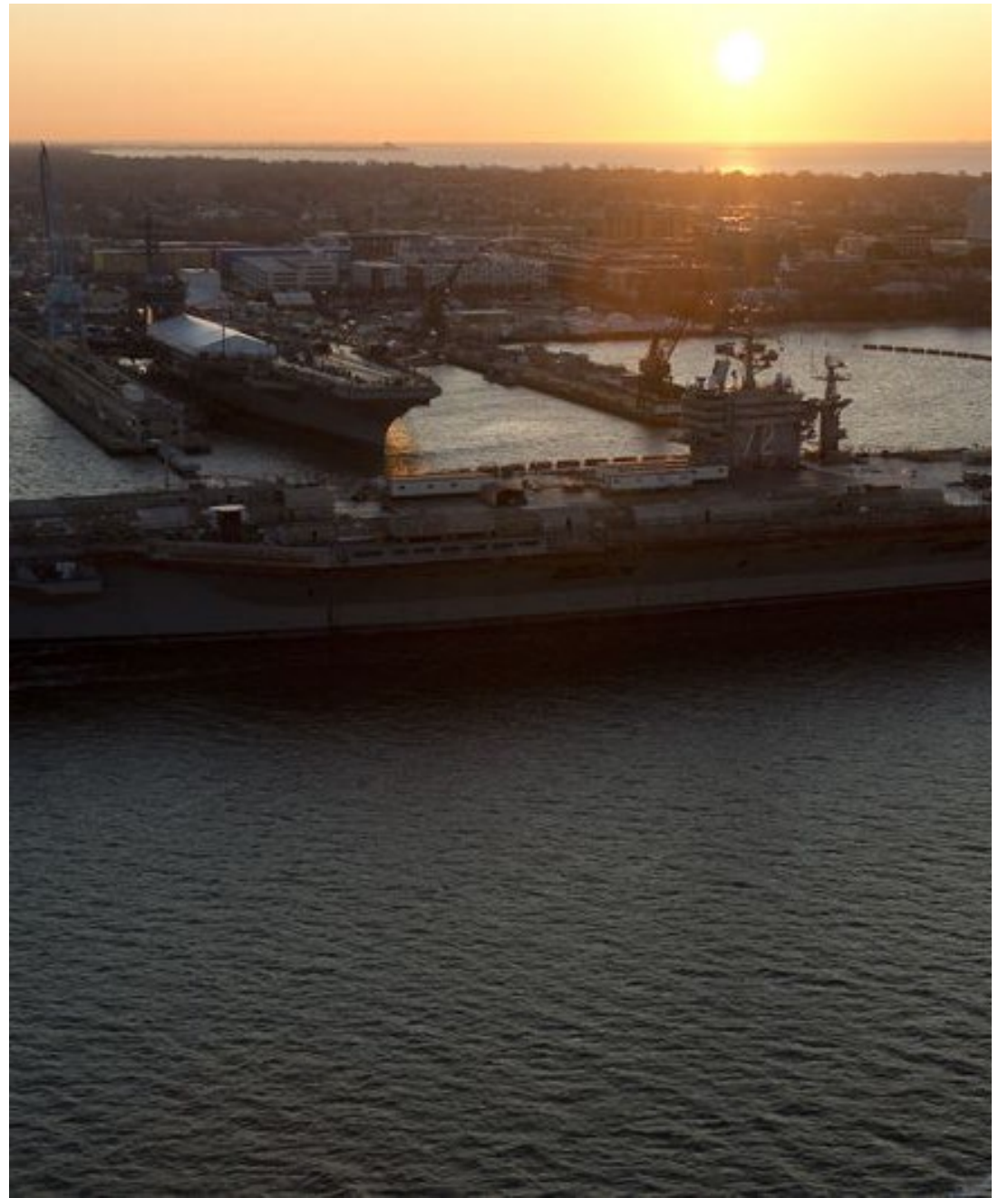
U-NNPI Authorized Computers and Electronic Transmission

- 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.



eProcurement Tools

- NNS has two eProcurement tools for NNS and Suppliers to communicate.
- Both SPARS and Exostar's Information Manager applications are **not authorized** for U-NNPI transmittals to, or from NNS.
- NNS Supplier Compliance has been notified of reoccurring instances and has started suspending accounts due to violations and will continue to monitor for additional violations.
- Please email Exostar@hii-nns.com to report any instances where you receive U-NNPI from NNS via one of these tools.



U-NNPI Control



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.

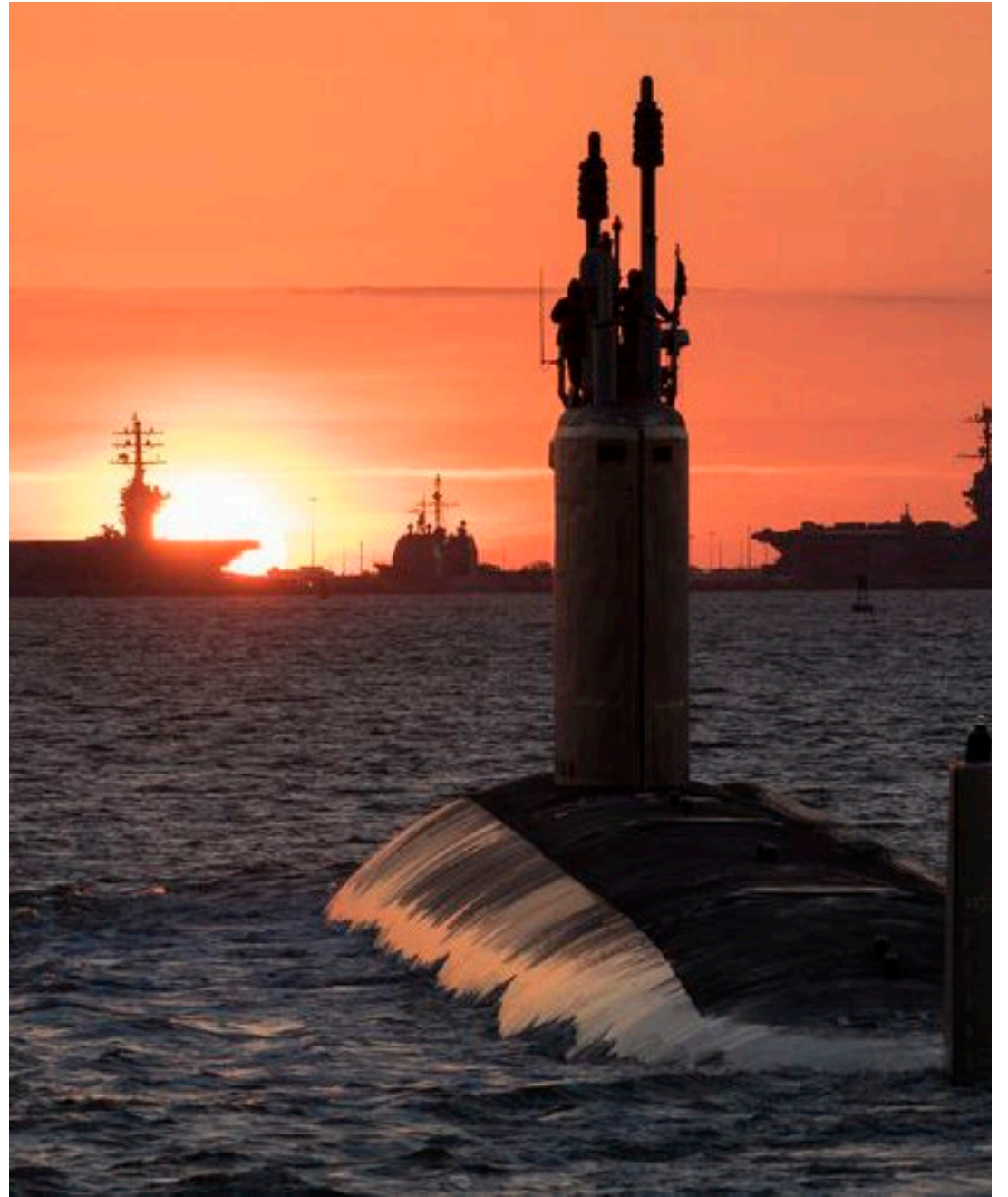
- Materials must remain under direct physical control by an authorized individual with NTK and in their personal possession.
- Must never be left unsecured, sent with checked baggage or left unattended in a vehicle
- Access to the space(s) where hardware is produced must be restricted to authorized individuals 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 -

Please add any questions in the chat box.

Thank you for attending today's webinar.

A PDF copy of the webinar will be posted to the NNS Supplier website before the end of the week.

