Questions from NNS Supplier Communication Webinar on Sensitive Information, Cybersecurity and Data Protection

Are you going to provide the slide deck after the Webinar?

The slide deck is available on the NNS External Supplier Website, under Important Announcements, which can be found at this link: https://hii.com/suppliers/newport-news-suppliers/nns-supplier-news-events/.

If I understand correctly, we cannot backup hard copy drawings mailed to us by scanning our network drawing folder. Is that correct?

That is correct. The NNS Buyer mails the drawings to the Supplier if the Supplier has not provided their NIST SP 800-171 controls implemented in Exostar for Cybersecurity assessment or Cybersecurity's assessment of current implemented controls dictates that the Supplier handle the drawings in hard copy only. If after the Supplier remains in hardcopy transmission status it means the self-assessment didn't meet HII-NNS's standards for cyber protection for the environment. Loading the document in the Supplier's information system negates Cybersecurity stance of hardcopy only. As the Supplier implements controls and submits updated information into Exostar, the Cybersecurity team reviews and modifies its recommendation to Supply Chain as appropriate.

If the Supplier has not completed the NIST SP 800-171 in Exostar and wishes to do so to potentially upgrade your company's status to permit electronic transmission, please reach out to the NNS Exostar team at Exostar@hii-nns.com.

Who needs the Exostar Information Manager application? Is it used for only specific kinds/types of contracts?

Exostar's Information Manager is available to all Suppliers and is approved to transmit commercial, DOD, and DOD-commercial procurement data up to, and including, Controlled Unclassified Information (CUI). NNS recommends all suppliers obtain the Exostar Information Manager application to ensure secure, faster transmission of documentation related to Federal Contract Information (FCI) and CUI.

In NNS' instance of Exostar's Information Manager, will there be an option to view the information within the application instead of downloading it first?

Currently NNS' instance of Exostar's Information Manager is set up to allow download and upload of documents. Document viewing is a feature being considered for future development.

If sub-tier suppliers also meet requirements for electronic CUI, are there any additional process steps needed for transmittal under a subcontract?

Suppliers should comply with all Purchase Order requirements that require flow down of terms for the transmission of electronic CUI if sub-tiers will receive CUI. This includes, but is not limited to, inclusion of DFARS 252.204-7012 in subcontracts. Higher-tier subcontractors are responsible for monitoring compliance with this clause at the sub-tier level.

If a supplier does not process FCI or] CUI, do they still have to complete the NIST SP 800-171 or any other questionnaire in Exostar's Onboarding Module (OBM)?

If the NNS Request for Quote (RFQ) and/or Purchase Order contain the DoD flowdowns, they have been assessed to contain at a minimum FCI; therefore, NNS recommends all suppliers complete the NIST SP 800-171 to get a determination for electronic transmission of FCI. If there are no DoD flowdowns in the Purchase Order terms and conditions, completion of the questionnaire is not required.

What are the JCP renewal requirements?

NNS' Webinar provided a snapshot overview of requirements outlined on the DLA's website. Refer to the DLA's JCP website at https://www.dla.mil/Logistics-Operations/Services/JCP/ for specific details as it relates to the renewal requirements.

If we have an approved JCP, do we need to resubmit a new application?

NNS' Webinar provided a snapshot overview of requirements outlined by the DLA. As long as your company maintains a valid active JCP, there is no requirement to submit a new application. The re-submittal is required for renewal as per the DLA's requirements. For more information, visit the DLA's website at https://www.dla.mil/Logistics-Operations/Services/JCP/.

Is there an equivalent to JCP for DIB suppliers not based within the U.S. or Canada?

The JCP was established to allow United States (U.S.)/Canadian contractors to apply for access to DoD unclassified export controlled technical data/critical technology. The program does not apply to suppliers from other countries. Foreign suppliers must work with their assigned Buyer to ensure information is exchanged in accordance with export control requirements.

As I understand it, the CMMC Level is required to be spelled out in a DoD contract. With that being a somewhat unknown, is there any guidance NNS can give a supplier on their expected CMMC compliance level based on a past work for NNS? It is not a simple matter to go from level 2 to 3, how do we avoid unexpected "surprises"?

Actual level will depend on the specifics of the contract and type of information that will be handled in future contracts. The best way to prepare for implementation of CMMC is to:

- Assess the type(s) of data your company has historically handled for NNS Purchase Orders (FCI, CUI, U-NNPI) as a general guide to the appropriate CMMC level. If FCI only, focus on CMMC Level 1. If CUI or U-NNPI, focus on CMMC level 2. NNS will share additional details on CMMC Level 3 as it becomes available from the DoD.
- Carefully conduct a self-assessment of your contractor-owned information systems to make sure you have implemented the necessary cybersecurity measures to comply with each requirement of FAR clause 52.204-21 or DFARS clause 252.204-7012.
- Review the appropriate security requirements and carefully consider whether they have been implemented to secure any contractor-owned information systems which will be used to process, store, or transmit DoD controlled unclassified information during contract performance.
- Before initiating an assessment, take corrective actions to meet any security requirements that necessitate implementation to comply with CMMC requirements.

Do I go to the Supplier Performance Risk System (SPRS) portal to do a Self-Assessment for a CMMC Level 2?

No. Contact the NNS Exostar team at Exostar@hii-nns.com to get started on the self-assessment requirements using the Exostar Onboarding Module. The Onboarding Module is where the NIST SP 800-171 CMMC Level 2 self-assessment is housed. SPRS is the location where your company would upload the score from the self-assessment for the government. Here is the link to SPRS: https://www.sprs.csd.disa.mil/.

For additional assessment information, please reference the CMMC Assessment Guide v. 2.13 at https://dodcio.defense.gov/Portals/0/Documents/CMMC/AssessmentGuideL2v2.pdf.

When do you see CMMC Phase 1 beginning?

Phase 1 begins at 48 CFR Rule Effective Date, which is expected Q2 2025.

When is HII planning to add CMMC requirements to contracts?

HII will add CMMC requirements to subcontracts when the subcontract involves Controlled Unclassified Information (CUI) or when the flow down requirements from HII's contract with DoD mandate that specific subcontractors meet specific CMMC levels. It is anticipated that this would be on the effective date of 48 CFR and the start of the phased roll-out. We will need to demonstrate compliance through self-assessments and/or third-party certification.

Is there a list available where DIB suppliers can find qualified C3PAOs?

The Cyber AB Marketplace is the authoritative source where you can find C3PAOs. Please visit https://cyberab.org/Catalog and filter by C3PAO.

Do the Prime and sub-contracts have to be the same level?

No, a lower CMMC level may apply to the subcontractor if the prime only flows down limited information. Additionally, the 32 CFR Final Rule includes a table outlining the requirements for situations where the organization seeking assessment (OSA) engages subcontractors to fulfill the contract. In such cases, subcontractors are required to meet a minimum CMMC status. The table is provided below for reference.

Table 2 – Minimum Flow-down Requirements

Prime Contractor Requirement	Minimum Subcontractor Requirement If the subcontractor will process, store, or transmit	
	FCI	CUI
Level 1 (Self)	Level 1(Self)	N/A
Level 2 (Self)	Level 1(Self)	Level 2 (Self)
Level 2 (C3PAO)	Level 1(Self)	Level 2(C3PAO)
Level 3 (DIBCAC)	Level 1(Self)	Level 2(C3PAO)

Is Exostar a requirement or optional for Suppliers?

Suppliers should comply with the Cybersecurity provision in the DoD appendices, which requires the Exostar OBM to report the status of a company's compliance with DFARS 252.204-7012, and more specifically the security requirements of NIST SP 800-171. The supplier is required to register and maintain an active account with Exostar OBM and to complete the Exostar OBM cybersecurity questionnaire. NNS instances of Exostar's Supply Chain Platform (SCP) and Information Manager (IM) are an optional service to provide expedited receipt of RFQ, POs, and file sharing in support of procurement activities.

How do I determine if a document is CUI?

There are ninety different CUI Categories, each with its own definition and its own set of regulatory requirements. The person generating the document needs to determine which Category applies to the information it contains. Depending on the content, it is possible that more than one Category may apply. The person generating the document then reviews the definitions applicable to each relevant Category to determine whether the actual content of the document falls within that definition.

Is HII-NNS fully compliant with the marking requirements for CUI/NNPI?

NNS is compliant with DODINST 5200.48 marking guidance for all CUI Categories other than NNPI.

NNS is fully compliant with the current NNPI marking guidance in OPNAVINST N9210.3, because that is the reference invoked by all of our prime contracts. NAVSEA (08) has not yet updated this marking guidance to match the standards for CUI set forth in DODINST 5200.48.

NAVSEA (08) has issued NNPPINST 5510.01, which will provide that updated guidance, but it is currently only applicable to Government stakeholders in the Naval Nuclear Propulsion Program (NNPP). This updated guidance will be flowed out to NNPP contractors and subcontractors via contract revisions when NAVSEA is ready to implement the change across the industrial base. NNS anticipates that the change is likely to occur sometime in 2025, but NAVSEA has not published a timeline for this.

If I already have my CMMC 2.0, DDTC, and Level 2 and JCP certification (exp. 2029), I should be pretty much all set, correct?

NNS is unable to provide guidance on whether any company is compliant. The requirements for CMMC compliance are company specific and the level of CMMC required is based on the information processed, stored, or transmitted.

If you are not signed up in BitSight will that reduce your vendor score?

No. Participation with the BitSight service is optional and will not reduce a supplier's score if not signed up. However, the tool is available at no cost to our suppliers and provides great information regarding observations of issues that the bad guys can see also. For those interested in an invitation to the service, please send your request to Ingalls.Exostar@hii-ingalls.com. This is a team shared mailbox managed by another HII division.

For international suppliers under the AUKUS agreement is hardcopy transmission of documents still an option?

Foreign suppliers must work with their assigned Buyer to ensure information is exchanged in accordance with export control requirements.

Is there a cost for accessing Exostar?

Yes. There is an annual fee of approximately $35 for the One Time Password (OTP) certificate that allows access into the application. Note that if you already have a Medium Assurance certificate, such as a Common Access Card (CAC), it can be used in lieu of the Exostar provided OTP.

Does CUI that does not rise to the need of JCP certification still require CMMC certification?

If your contract includes DFARS 252.204-7012 or involves CUI as defined by the DoD, you are required to achieve at least CMMC Level 2 certification for handling that information.

Where can I see a list of these markings, for FCI/CUI, U-NNPI?

Markings for NNPI are specified in OPNAVINST N9210.3.

Markings for CUI are specified in DODINST 5200.48, available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF. Additional marking guidance for some Categories is provided by the entry for each Category on the CUI Registry website found here: https://www.archives.gov/cui/registry/category-list.

If we already use Exostar and Shipbuilding Partners and Suppliers (SPARS), are we required to have access to BitSight?

No. Participation with the BitSight service is optional. However, the tool is available at no cost to our suppliers and provides great information regarding observations of issues that adversaries can also see.

Is it acceptable to treat all documents as CUI?

No, this is not acceptable. Treating your entire environment as though it processes, stores, and transmits Controlled Unclassified Information (CUI) may seem like a simpler approach, but it creates significant challenges during CMMC scoping and compliance efforts:

- Increased compliance burden
  - Drives up costs by securing systems that don't handle CUI
  - Expands the scope unnecessarily
- More complex assessments
  - Lengthens CMMC Certified Third Party Assessment Organization (C3PAO) assessments
  - Requires extra evidence for unrelated systems
- Reduced operational flexibility
  - Adds unnecessary controls for non-CUI tasks
  - Limits operational efficiency
- Misalignment with CMMC guidance
  - CMMC encourages scoping boundaries
  - Avoids over-securing non-CUI boundaries

A lot of CUI requirements don't apply to COTS items. As a small reseller of COTS items we are struggling with the requirements imposed on sub-tier vendors. Can COTS items be CUI? When a RFQ from NNS is coded CUI and it's a COTS item how are we supposed to know what exactly is CUI? We see the CUI statement on the quote but it's a COTS item and there are no attachments. The buyers can't answer what is CUI on the RFQ so how are we supposed to know what on the RFQ is CUI?

The most common CUI document associated with Purchase Orders (POs) is Appendix B (either App. B-DoD or App. B-662). The App. B is not attached to the PO; however, the vendor must request a copy from the Buyer. Other common CUI items are other Appendices, some drawings, P-Specs, and some Mil-specs.

What is the requirement for a vendor who does not handle CUI and does not expect to do so? How should they communicate this to NNS?

The term "handle" is an oversimplification. The accurate language for determining CMMC requirements revolves around whether a vendor processes, stores, or transmits Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). A supplier that does not process, store, or transmit CUI but does process, store, or transmit FCI will need to meet CMMC Level 1 requirements. Suppliers that do not process, store, or transmit FCI nor CUI may not require CMMC certification, but they should carefully review their contracts to confirm their obligations.

Is Cybersecurity Compliance and Risk Assessment (CCRA) replacing the Exostar?

Not at this time. DFARS 252.204-7012 requires compliance with the NIST SP 800-171 controls. As we advance to the CMMC requirements, we will review the appropriate requirements going forward, which may include the CCRA assessment.

If someone sends us a physical product, and does not mention CUI, how would we know if pictures of that product count as CUI?

If NNS forwards CUI material to your company with photos or pictures of the product, then it should be labeled as CUI before you open the material.

When is HII planning on having their scheduled C3PAO assessment (roughly)? What is the assumed lag time between the HII assessment certification and its suppliers requiring a C3PAO certification?

There is no universally defined lag timeframe, but preparing for C3PAO assessments could take several months. We encourage suppliers to review their current compliance status and begin preparations to ensure they are ready for certification when required. Early readiness efforts can help avoid delays and ensure alignment with contract timelines.

- Timing largely depends on contract requirements.
- For higher priority or time-sensitive contracts, timelines may be shorter.
- Keep in mind the plan of actions and milestones (POA&M) when building your timelines. All requirements scored "NOT MET" and placed on the POA&M must be remediated within 180 days of receiving the conditional CMMC status, and Final Level 2 Certification will not be awarded until successful POA&M closeout assessment.

What CMMC level does NNPI invoke?

While NNPI is a type of CUI that requires specific security measures, the specific CMMC level required for handling NNPI can vary depending on the contract and the sensitivity of the information involved.

At what Phase will we need to meet all controls for CMMC without any POA&Ms?

Essentially, contract award is the phase where all applicable controls must be met without relying on a plan of action and milestones (POA&M), but this depends on the specific CMMC level and contract requirements.

Organizations Seeking Assessment (OSAs) that have met all 15 Level 1 requirements have achieved CMMC Status of Final Level 1 (Self). There are no POA&Ms for Level 1. The OSA must submit an affirmation of compliance with FAR clause 52.204-21 requirements in Supplier Performance Risk System (SPRS). At this point, OSAs have satisfied the CMMC requirements needed for award of contracts requiring a CMMC Status of Final Level 1 (Self). To maintain a CMMC Status of Final Level 1 (Self), this entire process must be repeated in full on an annual basis, including both self-assessment and affirmation.

For Level 2 assessments, if all 110 requirements are satisfied, the assessment score will be 110 and the OSA will have achieved a CMMC Status of Final Level 2 (Self) or Final Level 2 (C3PAO) as applicable and is eligible for contract award as long as all other contractual requirements are met.

Not all requirements must immediately be MET to be eligible for contract award. If the minimum score is achieved on the assessment (equal to 80% of the maximum score) and certain critical requirements are met, OSAs will achieve a CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO) as applicable. All NOT MET requirements must be noted in an assessment Plan of Action and Milestones (POA&M). At this point the OSA will have satisfied the CMMC requirements needed for contract award OSAs must have met all 110 security requirements of NIST SP 800-171 R2 within 180 days of receiving their Conditional CMMC Status, which must be verified with a second assessment, called a POA&M closeout assessment. If the POA&M closeout assessment finds that all requirements have been met, then the OSA will achieve a CMMC Status of Final Level 2 (Self) or Final Level 2 (C3PAO) as applicable. However, if a POA&M closeout assessment does not find that all requirements have been met by the end of 180 days, then the CMMC Status of Conditional Level 2 (Self) or Conditional Level 2 (C3PAO) will expire. At this point, standard contractual remedies will apply.

My company's ERP does not support the current versions of Windows yet, how can we ever meet these requirements?

If your Enterprise Resource Planning (ERP) system does not support current versions of Windows, there are a few considerations to address this within the context of CMMC and NIST SP 800-171 requirements. Unsupported operating systems can pose security risks, as they may no longer receive updates or patches, which could affect compliance for systems handling Controlled Unclassified Information (CUI).

Organizations in this situation may explore ways to mitigate risks by documenting any compensating controls or interim measures within their System Security Plan (SSP). Reviewing options with ERP

vendors to understand upgrade or mitigation paths is another potential avenue, as is ensuring robust security practices for the current system while a transition plan is developed.

If we provide services only how would we know the equipment we work on and the documents we create would be CUI?

- Check your contracts for clauses like FAR 52.204-21, which applies to systems handling FCI.
- Check your contracts for references to DFARS 252.204-7012, which applies to systems handling CUI.
- Check for markings or designations – FCI is not typically labeled, but CUI should be explicitly marked in documents or communications.
- Consult with your contracting officer or program manager for clarification on whether the information is FCI or CUI.
- Assess your systems and processes to determine what data and information falls under federal safeguarding requirements.

If a drawing is not marked CUI, but has a distribution statement D, must the sub-tier supplier who receives it be CMMC certified? If so, what level? If the supplier is not certified, can the supplier receive the data via fax as long as they do not upload it to their network?

Distribution Statement D is one of the many legacy markings that fall under the CUI umbrella. Existing documents bearing Distribution Statement D markings should be treated as CUI//EXPT, but do not need to be re-marked until/unless they are modified for some other reason.

Distribution D information can only be shared with JCP-certified contractors and with the Government.

If technical information from a Distribution D document is incorporated into a new document, the new document should be marked as CUI//EXPT.

Is a medium assurance certificate still required for incident reporting? According to 32 CFR Part 236 it is not required and a PIEE account would work for incident reporting. Also, are External Service Providers able to submit cyber incidents on behalf of an org?

The CMMC program is designed only to validate implementation of the information security standards in FAR clause 52.204-21, NIST SP 800-171 R2, and a selected subset of NIST SP 800-172 Feb2021. This rule does not address the other DFARS clause 252.204-7012 requirements for cyber incident reporting. The CMMC assessment framework will not alter, alleviate, or replace the cyber incident reporting aspects of DFARS clause 252.204-7012, which will remain effective where applicable.

Does the receipt of U-NNPI via hard copy or fax affect the Level of CMMC required for a supplier?

If a supplier processes, stores, or transmits any form of CUI, including receiving faxes, CMMC likely applies, but this depends on contract requirements, and whether or not the information falls within the defined scope. Reviewing the contract is essential for determining the exact CMMC level requirement.

Will hard copies be phased out in the next few years?

We can’t phase out hard-copies for CUI unless/until the Supplier in question meets the requirements of NIST 800-171 and DFARS Clause 252.204-7012.

We can't phase out hard-copies for U-NNPI unless and until the Supplier obtains Authority to Operate (ATO) from NAVSEA 08.

Aside from being CMMC "certified" by a 3rd party, is there an official entity that does certification?

The official path to CMMC certification is through a CMMC Third-party Assessment Organization (C3PAO) authorized by the Cyber Accreditation Body (Cyber AB). While the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) may assess certain high-priority contractors, it does not function as a standard certification body for the broader DIB.

Are there any dates established for the phases?

Expect 32 CFR, which establishes CMMC as a program, to have an effective date of December 16, 2024, and anticipate 48 CFR, which implements CMMC into contracts, in Q2 of 2025. This projection is based on the closing of the public comment period on October 15, 2024 for the 48 CFR Proposed Rule. We know the phased implementation of CMMC will roll out over 36 months with Phase 1 starting on the effective date of 48 CFR, Phase 2 following 12 months of the effective date of 48 CFR, Phase 3 following 24 months of the effective date of 48 CFR, and full roll-out 36 months after the effective date of 48 CFR.

There was mention that all of these changes were going to affect "award" of contracts. Does that mean that any contracts already awarded will not have to meet these requirements, including future material procurement from sub tiers?

One of the main purposes of the CMMC Program is to ensure that DoD contracts that require contractors to safeguard CUI will be awarded to contractors with the ability to protect that information. All contractor-owned information systems that process, store, or transmit CUI are subject to the requirements of NIST SP 800-171 when DFARS clause 252.204 7012 is included in the contract. Meaning, if your awarded contract includes this clause (today), you are already required to implement the required security controls.

Obtaining a CMMC certification through C3PAO assessment applies to the authorization boundary (or CUI boundary) defined in your assessment. This means the certification will cover all systems and processes within that boundary, ensuring compliance for all applicable contracts involving CUI within that scope.

It should also be noted the DoD may include CMMC requirements on contracts awarded prior to 48 CFR part 204 CMMC Acquisition rule becoming effective, but doing so will require bilateral contract modification after negotiations, as stated in the Federal Register: Cybersecurity Maturity Model Certification (CMMC) Program found at this file path: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program.

How do we know if we have FCI or CUI?

- Check your contracts for clauses like FAR 52.204-21, which applies to systems handling FCI.
- Check your contracts for references to DFARS 252.204-7012, which applies to systems handling CUI.
- Check for markings or designations – FCI is not typically labeled, but CUI should be explicitly marked in documents or communications.
- Consult with your contracting officer or program manager for clarification on whether the information is FCI or CUI.
- Assess your systems and processes to determine what data and information falls under federal safeguarding requirements.