Newport News Shipbuilding
A Division of HII

memo

To: All Valued Suppliers

From: Supplier Compliance

Date: 09/23/2022

Subject: Safeguarding Unclassified Navel Nuclear Propulsion Information (U-NNPI)

The purpose of this memo is to increase our supplier's awareness and understanding of the requirements invoked in Newport News Shipbuilding (NNS) purchase orders that include U-NNPI. Safeguarding this information is a requirement of having access to U-NNPI and **critical to our national security**. If after reviewing this document you still have questions, please reach out to NNSSupplierNotification@hii-nns.com.

U-NNPI is Unclassified Naval Nuclear Propulsion 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. **OPNAV Instruction N9210.3 is the guidance document** 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. The document contains definitions, marking requirements, control and storage requirements, information disclosure policy, allowance of facility visits, etc.; suppliers are required to meet these requirements to be in compliance with purchase orders that include U-NNPI.

Supplier Requirements to Receive NNPI

- Valid **Need-to-Know (NTK)**
- Valid Commercial and Government Entity **(CAGE)** / North Atlantic Treaty Organization (NATO) Commercial and Government Entity **(NCAGE).** The information recorded for the CAGE must exactly match the information entered on the DD Form 2345.
- Current and Active System for Award Management **(SAM)** registration
- National Institute of Standards and Technology **(NIST)** Assessment documented in the ***Supplier Performance Risk System (SPRS)*** prior to submitting your JCP Application. **Effective 30 November 2020**, the Defense Federal Acquisition Regulation Clause 252.204-7012 requires all DOD contractors and subcontractors to implement cybersecurity requirements in the NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Failure to have a NIST assessment documented in SPRS will result in a denial of the request for an approved DD Form 2345.
- Active Joint Certification Program **(JCP)** – The Joint Certification Program (JCP) certification establishes the eligibility of a United States (U.S.) or Canadian contractor to receive technical data governed, in the U.S., by Department of Defense (DOD) Directive 5230.25 and, in Canada, by the Technical Data Control Regulations (TDCR). Certification is required for United States (U.S.) or Canadian contractors who wish to obtain access to unclassified technical data disclosing militarily

critical technology with military or space application that is under the control of, or in the possession of the U.S. Department of Defense (DOD) or the Canadian Department of National Defense (DND).
- Annually complete Form NN 9540, *Security Agreement for Protection of NNPI;* the physical address the Supplier receives U-NNPI must match the JCP address. If address does not match, there should be a reasonable explanation for the difference.

Safeguarding and Storage Requirements

- U-NNPI shall be controlled so that those without a NTK cannot obtain visual or physical access that would permit detailed examination.
  - 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 U-NNPI documents are in the custody of an authorized individual using them:
  - This individual must prevent detailed visual or physical access by those who do not have an NTK.
  - Any time U-NNPI is not in the direct control of an authorized person, it should be stored in a key lock container, ex. file cabinet, desk, and/or safe.
- Supplier must have a documented Key Control Process for the key to the container where NNPI is stored; when not in use.
- Only authorized persons may have access to the container.
- Compromise of the container must be obvious at sight.
- Container should not have any external labels indicating the sensitivity of the contents.
- 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 each page.
- Attach a cover sheet to display the following warning statement:
  - 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
- 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.
- If removed from the Supplier's facility, U-NNPI must remain in the personal possession of an authorized person at all times.
  - U-NNPI must never be left unsecured
    - Sent with checked baggage
    - Left unattended in an automobile or hotel room.

DISCLAIMER: The information contained herein should be used to highlight specific guidance and should not be used as a replacement for reading the entire OPNAV Instruction N9210.3 to ensure compliance with **all** of the applicable requirements.