

NNPI (Unclassified) — Naval Nuclear Propulsion Information Protection Requirements



NNPI Protection Requirements establish controls to safeguard Naval Nuclear Propulsion Information from unauthorized disclosure and misuse.

What it is

U.S. NNPI (Unclassified) — Naval Nuclear Propulsion Information Protection Requirements is a regulatory framework that guides organizations in safeguarding unclassified Naval Nuclear Propulsion Information (NNPI) against unauthorized disclosure and misuse. Its primary purpose is to establish security controls to protect sensitive information related to the U.S. Navy’s nuclear propulsion programs, even when the data is unclassified.

The framework is published and enforced by the U.S. Department of the Navy, specifically overseen by the Naval Nuclear Propulsion Program (Naval Reactors). It applies to contractors, civilian personnel, and other entities handling NNPI, covering a range of areas including information security, classification management, employee training, and compliance oversight.

At a glance

PUBLISHER U.S. Department of the Navy (specifically, Naval Reactors within the Department of the Navy) ([law.cornell.edu] (https://www.law.cornell.edu/cfr/text/32/117.23?utm_source=openai))	TYPE Regulation	VERSION NN-801 (March 2022) Revision 05
EFFECTIVE March 26, 2024	DOMAIN Quality & Safety	FAMILY Other
REGION United States	INDUSTRY Aerospace & Defense	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://www.secnav.navy.mil/doni/Directives/09000%20General%20Ship%20Design%20and%20Support/09-200%20Propulsion%20Plants%20Support/N9210.3%20%28Unclass%20Portion%29.pdf>

Why it matters

- Enhance regulatory alignment** Support compliance with Department of the Navy mandates and federal standards, reducing legal and operational risks for organizations handling NNPI.
- Strengthen data protection practices** Increase control over sensitive information by defining access restrictions and labeling requirements tailored to defense-related data.
- Improve internal security oversight** Enable organizations to proactively manage information security through structured processes, employee training, and regular compliance monitoring.
- Promote operational resilience** Reduce the likelihood and impact of data leaks or unauthorized disclosure by instituting

How SmartSuite supports NNPI

NNPI Information Protection Library

Structure policies and safeguards governing handling, storage, and transmission of Naval Nuclear Propulsion Information.

Controlled Information Inventory

Track systems, repositories, and documents containing NNPI to ensure proper protection and oversight.

Personnel Authorization and Access Governance

Manage workforce authorization, role assignments, and access controls for individuals handling NNPI.

NNPI Encryption and Transfer Controls

Track encryption requirements, data transfer approvals, and secure communication practices for NNPI.

NNPI Disclosure Risk Monitoring

Monitor potential disclosure risks and track response workflows for NNPI security incidents.

NNPI Control and Security Oversight Readiness Reporting

Provide dashboards summarizing NNPI control implementation status, access governance, and security oversight readiness.

Common framework mappings

CIS Controls v8.1

COBIT 2019

DFARS 252.204-7012

NIST 800-171 Rev. 3

FedRAMP Rev. 5

ISO 27001:2022

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

CMMC 2.0

Official resources

Naval Nuclear Propulsion Information Protection Requirements

Defines requirements for safeguarding unclassified Naval Nuclear Propulsion Information.
secnav.navy.mil/doni/Directives/09000%20General%20Ship%20Design%20and%20Support/09-200%20Propulsion%20Plants%20Support/N9210.3%20%28Unclas%20Portion%29.pdf

NISPOM (National Industrial Security Program Operating Manual)

Outlines security requirements for contractors dealing with classified information.
exwc.navfac.navy.mil/Portals/88/Documents/EXWC/DoD_Locks/PDFs/NISPOM.pdf

Frequently asked questions

What is the U.S. NNPI (Unclassified) Protection Requirements framework used for?

The U.S. NNPI (Unclassified) Protection Requirements framework is designed to safeguard unclassified Naval Nuclear Propulsion Information against unauthorized disclosure and misuse. It establishes mandatory security controls to protect sensitive information related to the Navy’s nuclear propulsion programs.

Is compliance with U.S. NNPI (Unclassified) Protection Requirements mandatory?

Yes, compliance is mandatory for all contractors, civilian personnel, and organizations handling Naval Nuclear Propulsion Information, as enforced by the U.S. Department of the Navy under the Naval Nuclear Propulsion Program (Naval Reactors).

Who does the U.S. NNPI (Unclassified) framework apply to?

The framework applies to any entity—including government personnel, contractors, and third parties—that handles, processes, stores, or transmits unclassified NNPI. Its scope covers both digital and physical information environments.

What key concepts or artifacts are required by U.S. NNPI (Unclassified) Protection Requirements?

Key artifacts include documented classification assessments, access control lists, employee training records, data labeling procedures, and incident response plans. Maintaining up-to-date compliance documentation is a core requirement.

How do organizations implement the NNPI (Unclassified) Protection Requirements?

Organizations implement NNPI requirements by integrating specific security controls on information handling, restricting access, labeling NNPI, conducting personnel training, and performing regular risk assessments and audits to ensure continuous protection.

How do NNPI Protection Requirements relate to other cybersecurity frameworks?

While NNPI requirements are unique to Naval Nuclear Propulsion Information, they align with broader federal regulations such as NIST and DFARS. Organizations often integrate NNPI controls into their general risk management and security compliance programs for comprehensive protection.

What are the ongoing compliance requirements for U.S. NNPI (Unclassified)?

Ongoing compliance involves regular audits, continuous monitoring of information handling practices, periodic employee training, maintenance of access and classification records, and timely incident reporting. Organizations must proactively update controls to address evolving risks.

How would SmartSuite support U.S. NNPI (Unclassified) Protection Requirements?

SmartSuite can centralize and streamline NNPI compliance management by providing risk tracking, control libraries specific to NNPI requirements, and evidence collection tools. The platform supports audit readiness with automated monitoring, reporting dashboards, and remediation workflows to help organizations maintain continuous oversight and compliance with NNPI Protection Requirements.

License included / downloadable: Yes NNPI unclassified protection guidance is available from official government publications. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/us-nnpi-unclassified-naval-nuclear-propulsion-information-protection-requirements