IT CHECKLIST FOR NNPI

1. IDENTIFICATION (ALL REQUIRED)

		Date Prepare:
Site Identification(UIC, PLA, or PSI):	C & A Package Identification (IATS or CAST Number):	
IT System Name:	Acronym for IT System (if one is used):	
IT System Identifier (DADMS ID #, DITPR-DON ID #, or Unique Network Name in DADMS):		
IT System Description:		
IA Manager (IAM)		
Name:	Phone Number:	E-mail Address:
Project or Program Manager		
Name:	Phone Number:	E-mail Address:

2. TYPE (CHOOSE ONE)

☐ **Information Systems** - Requirements in chapters 1-10 and 11 of OPNAVINST N9210.3 shall be met. See Chapter 11 paragraph 3a(2) of OPNAVINST N9210.3 for additional detail on this form and required supporting documentation.

☐ **Telecommunication Systems** - Requirements in chapters 1-10 and 12 of OPNAVINST N9210.3 shall be met. This checklist provides comprehensive guidelines for items to be addressed regarding control and protection for NNPI on IT. The NNPI control categories addressed and controls selected shall be tailored as appropriate for security plans for telecommunication systems processing or that are planned to process NNPI that are submitted to CNO (N00N) for approval or information.

☐ **Other Electronics** - Requirements in chapters 1-10 and 13 of OPNAVINST N9210.3 shall be met. This checklist provides comprehensive guidelines for items to be addressed regarding control and protection for NNPI. The NNPI control categories addressed and controls selected shall be tailored as appropriate for security plans for electronics (not otherwise addressed as an information system or telecommunication system) processing or that are planned to process NNPI that are submitted to CNO (N00N) for approval or information.

3. CLASSIFICATION (CHOOSE ONE)

☐ Unclassified naval nuclear propulsion information (U-NNPI)
All NNPI security control requirements in 5.1 through 5.18 of this checklist apply.

☐ Classified naval nuclear propulsion information
All NNPI security control requirements in 5.1 through 5.17 and 5.19 of this checklist apply.

4. SECURITY CONTROL CATALOG (CHOOSE ONE OR BOTH)

☐ DOD Instruction 8500.2 of 6 Feb 03 (or subsequent version)

☐ NIST Special Publication 800-53 ver. 3 of Aug 09 (or subsequent ver.)

5. NNPI CONTROL REQUIREMENTS (CHECK IF COMPLIES)

5.1. ACCESS CONTROL (AC)

☐ 5.1.1 Controls are implemented/maintained to limit NNPI access to authorized NNPI users, to processes acting on behalf of authorized users or devices (including other information systems), and to the types of transactions and functions authorized users are permitted to exercise.

☐ 5.1.2 Controls are implemented/maintained to limit NNPI access with hardware and system configurations in such a manner that the IT users may not compromise them.

5.2. AWARENESS AND TRAINING (AT)

☐ 5.2.1 Controls are implemented/maintained to ensure that managers and users of the information systems processing NNPI know about the security risks associated with their activities and the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of information systems and NNPI.

☐ 5.2.2 Controls are implemented/maintained to ensure that personnel are adequately trained to carry out their assigned NNPI information security-related duties and responsibilities.

☐ 5.2.3 Controls are implemented/maintained to ensure that all NNPI users receive initial and annual refresher NNPI training. Records of training for the most recent training received by users shall be retained.

☐ 5.2.4 Controls are implemented/maintained to ensure that each NNPI users has a signed user agreement on record prior to being granted access to NNPI on the information system.

5.3. AUDIT AND ACCOUNTABILITY (AU)

☐ 5.3.1 Controls are implemented/maintained to create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity involving NNPI.

☐ 5.3.2 Controls are implemented/maintained to ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

5.4. CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS (CA)

☐ 5.4.1 NNPI controls on the information system are periodically (at least annually) assessed to determine if the controls are effective.

☐ 5.4.2 Controls are implemented/maintained to ensure that privileged users develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities to unauthorized disclosure or spillage of NNPI on the information system.

☐ 5.4.3 Controls are implemented/maintained to ensure that only authorized information systems interconnection(s) are implemented.

☐ 5.4.4 Information system security controls for NNPI are monitored on an ongoing basis to ensure the continued effectiveness of the controls.

5.5. CONFIGURATION MANAGEMENT (CM)

☐ 5.5.1 NNPI controls are implemented/maintained on the information system to establish and maintain baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

☐ 5.5.2 NNPI controls are implemented/maintained on the information system to establish and enforce security configuration settings for information technology products employed in information systems.

5.6. CONTINGENCY PLANNING (CP)

☐ 5.6.1 NNPI controls are incorporated into organizational efforts to establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for information systems to ensure the availability of critical information resources (including NNPI) and continuity of operations in emergency situations.

5.7. IDENTIFICATION AND AUTHENTICATION (IA)

☐ 5.7.1 Controls are implemented/maintained to identify NNPI information system users, processes acting on behalf of NNPI users, or NNPI devices and authenticate (or verify) the identities of those authorized NNPI users, processes, or devices, as a prerequisite to allowing access to NNPI on information systems.

5.8. INCIDENT RESPONSE (IR)

☐ 5.8.1 Controls are implemented/maintained for an operational NNPI incident handling capability for information systems that include adequate preparation, detection, analysis, containment, recovery, and user response activities.

☐ 5.8.2 Controls are implemented/maintained to track, document, and report NNPI incidents to appropriate organizational officials and/or authorities (such as the DAA).

☐ 5.8.3 Controls are implemented/maintained for verifying the occurrence of unauthorized or inadvertent disclosures of NNPI and reporting verified incidents to the Operational DAA and CNO (N00N). Suspected Unauthorized or inadvertent disclosures of U-NNPI shall be verified and reported, if confirmed, within 24 hours. Unauthorized or inadvertent disclosures of classified NNPI shall be verified and reported, if confirmed, within 8 hours.

☐ 5.8.4 Controls are implemented/maintained for responding to and resolving incidents of unauthorized or inadvertent disclosures of NNPI. U-NNPI incidents shall be resolved and closed within 30 calendar days of initial reporting. Classified NNPI incidents shall be resolved within 14 calendar days of initial reporting.

5.9. MAINTENANCE (MA)

☐ 5.9.1 Controls are implemented/maintained to perform periodic and timely maintenance on information systems involving NNPI.

☐ 5.9.2 Controls are implemented/maintained for the tools, techniques, mechanisms, and personnel used to conduct information system maintenance to preclude foreign national or unauthorized access to NNPI.

5.10. MEDIA PROTECTION (MP)

☐ 5.10.1 Controls are implemented/maintained to protect NNPI on information system equipment and IT media.

☐ 5.10.2 Controls are implemented/maintained to limit access to NNPI on IT media to authorized NNPI users.

☐ 5.10.3 Controls are implemented/maintained to dispose of NNPI IT media per chapter 6 of OPNAVINST N9210.3.

☐ 5.10.4 Controls are implemented/maintained to ensure that NNPI IT media is disposed of when no longer needed or accumulated for disposal at a periodicity not longer than a calendar year.

☐ 5.10.5 Controls are implemented/maintained to ensure that unattended IT media containing NNPI (classified or unclassified) has adequate physical protections commensurate with the level of information they contain.

☐ 5.10.6 Controls are implemented/maintained for ingress and egress controls for NNPI IT media and equipment per OPNAVINST N9210.3 and DAA policy.

☐ 5.10.7 Controls are implemented/maintained to ensure that IT media used to transfer NNPI to or from information systems accredited for NNPI are used only for required business/work purposes and are not used to introduce malicious code, vulnerabilities, or mechanisms for the collection or redirection of information processed on the information system.

☐ 5.10.8 Controls are implemented/maintained to ensure that IT media used for NNPI are only used on information systems with an accreditation for NNPI commensurate with the highest level and most restrictive controls required for the IT media. Reuse of IT media containing NNPI on a less restrictive or low classification of information system is prohibited.

5.11. PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

☐ 5.11.1 Controls are implemented/maintained to prevent physical access to information systems, equipment, IT media, and the respective operating environments involving NNPI by foreign nationals or others without a need-to-know per OPNAVINST N9210.3.

☐ 5.11.2 Controls are implemented/maintained to protect the physical plant and support infrastructure for information systems processing NNPI.

☐ 5.11.3 Controls are implemented/maintained to limit physical access to NNPI IT resources in manner that is commensurate with the classification and handling requirements for the information processed. These controls shall be in place to prevent unauthorized physical access, tampering, damage, and theft. This can be achieved by controlling access into specific areas or by controlling access to specific resources (e.g., PCs, printers, servers, network devices, wiring closets, etc).

5.12. PLANNING (PL)

☐ 5.12.1 Controls are implemented/maintained to develop, document, periodically update, and implement security plans for information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing NNPI.

5.13. PERSONNEL SECURITY (PS)

- ☐ 5.13.1 Controls are implemented/maintained to ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria (including NNPI) for those positions.
- ☐ 5.13.2 Controls are implemented/maintained to ensure that NNPI and information systems are protected during and after personnel actions such as terminations and transfers.
- ☐ 5.13.3 Controls are implemented/maintained to employ formal sanctions for personnel failing to comply with organizational security policies and procedures regarding NNPI.

5.14. RISK ASSESSMENT (RA)

- ☐ 5.14.1 Controls are implemented/maintained to periodically assess the risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of information systems and the associated processing, storage, or transmission of NNPI.

5.15. SYSTEM AND SERVICES ACQUISITION (SA)

- ☐ 5.15.1 Controls are implemented/maintained to allocate sufficient resources to adequately protect information systems with regards to NNPI processing needs.
- ☐ 5.15.2 Controls are implemented/maintained to employ system development life cycle processes that incorporate NNPI information security considerations.
- ☐ 5.15.3 Controls are implemented/maintained to employ necessary software usage and installation restrictions regarding NNPI processing.
- ☐ 5.15.4 Controls are implemented/maintained to ensure that third-party providers employ adequate NNPI security measures to protect infor applications, and/or services outsourced from the organization.

5.16. SYSTEM AND COMMUNICATIONS PROTECTION (SC)

- ☐ 5.16.1 Controls are implemented/maintained to monitor, manage, and protect organizational communications (i.e., information transmitted or received by information systems) at the external boundaries and key internal boundaries of the information systems processing NNPI.
- ☐ 5.16.2 Controls are implemented/maintained to employ architectural designs, software development techniques, and systems engineering printhat promote effective NNPI security within information systems.

5.17. SYSTEM AND INFORMATION INTEGRITY (SI)

- ☐ 5.17.1 Controls are implemented/maintained to identify, report, and correct information and information system flaws affecting NNPI related controls in a timely manner.
- ☐ 5.17.2 Controls are implemented/maintained to provide protection from malicious code at appropriate locations within information system processing NNPI.
- ☐ 5.17.3 Controls are implemented/maintained to monitor information system security alerts and advisories for NNPI and take appropriate actions in response.

5.18. U-NNPI SPECIFICATIONS (U-NNPI SYSTEMS ONLY)

- ☐ 5.18.1 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for data in transit on information systems used to process up to U-NNPI.
- ☐ 5.18.2 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for data at rest on mobile client devices processing up to U-NNPI.
- ☐ 5.18.3 Controls are implemented/maintained to ensure an FIPS-140-2 certified encryption is implemented for all removable IT media (including peripheral electronic storage) containing up to U-NNPI. IT media includes, but is not limited to, optical media (such CDs or DVDs), universal serial bus (USB) thumb drives, and external hard-drives.
- ☐ 5.18.4 Controls are implemented/maintained to ensure that IT equipment, media, electronic displays, and other IT items for U-NNPI are marked or labeled per chapter 2 of OPNAVINST N9210.3.
- ☐ 5.18.5 Controls are implemented/maintained to ensure that U-NNPI IT media and equipment are disposed of per chapter 6 of OPNAVINST N9210.3.
- ☐ 5.18.6 Controls are implemented/maintained to ensure that users are prompted to accept the following terms during the initial logon for each session that includes access to U-NNPI:

  You are approved to process up to and including unclassified naval nuclear propulsion information (U-NNPI) on this system.

  U-NNPI is not for release to foreign nationals (NOFORN) and has special handling requirements. U-NNPI is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of the Director, Naval Nuclear Propulsion Program (CNO (N00N)). *It is your responsibility to protect U-NNPI from disclosure to individuals without a need-to-know.*

  You are not approved to process classified information on this system.

5.19. CLASSIFIED NNPI SPECIFICATIONS (CLASSIFIED NNPI SYSTEMS ONLY)

- ☐ 5.19.1 Controls are implemented/maintained to ensure a NSA Type 1 certified encryption is implemented for data in transit or protected distribution systems are used per the requirements of NSTISSI No. 7003 of 13 Dec 96, Protective Distribution Systems (PDS) on information systems used to process classified NNPI.
- ☐ 5.19.2 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for data at rest on mobile client devices processing classified NNPI until an NSA Type 1 certified encryption product for data at rest is available, at which time the NSA Type 1 certified encryption product shall be used for data at rest on mobile client devices processing classified NNPI.

☐	5.19.3 Controls are implemented/maintained to ensure a FIPS-140-2 certified encryption is used for all removable IT media (including peripheral electronic storage) containing classified NNPI until an NSA Type 1 certified encryption product for data at rest is available, at which time the NSA Type 1 certified encryption product shall be used for all removable IT media (including peripheral electronic storage) containing classified NNPI. IT media includes, but is not limited to, optical media (such CDs or DVDs), universal serial bus (USB) thumb drives, media cards, and external hard-drives.
☐	5.19.4 Controls are implemented/maintained to ensure that IT equipment, media, electronic displays, and other IT items for classified NNPI are marked or labeled per chapter 2 of OPNAVINST N9210.3.
☐	5.19.5 Controls are implemented/maintained to ensure that classified NNPI IT media and equipment are disposed of per chapter 6 of OPNAVINST N9210.3.
☐	5.19.6 Controls are implemented/maintained to ensure that a classified NNPI user on IT systems authorized up to the CONFIDENTIAL or SECRET level are prompted to accept the following terms during the initial logon for each session that includes access to classified NNPI: *You are approved to process up to and including* [*CONFIDENTIAL* or *SECRET* as appropriate] *naval nuclear propulsion information (NNPI) on this system.* *NNPI is not for release to foreign nationals (NOFORN) and has special handling requirements.* NNPI is subject to special export controls, and each transmittal to foreign governments or foreign nationals may be made only with the approval of the Director, Naval Nuclear Propulsion Program (CNO (N00N)). *It is your responsibility to protect NNPI from disclosure to individuals without a need-to-know.* *Access to RESTRICTED DATA (RD) NNPI requires FINAL Government clearance. It is your responsibility to protect RD NNPI from disclosure to individuals without a final clearance.*

6. Acknowledgement. The undersigned certifies that the information system referenced on this checklist meets Security Control Requirements for U-NNPI or classified NNPI (as appropriate), as listed in OPNAVINST N9210.3.

Name:	Title:
Signature:	Date: