

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
<i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				a. FACILITY CLEARANCE REQUIRED SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED SECRET	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>			3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>		
a. PRIME CONTRACT NUMBER		X	a. ORIGINAL <i>(Complete date in all cases)</i>		DATE (YYYYMMDD) 20120501
b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO.	DATE (YYYYMMDD)
X	c. SOLICITATION OR OTHER NUMBER N00039-12-R-0009	DUE DATE (YYYYMMDD)	c. FINAL <i>(Complete Item 5 in all cases)</i>		DATE (YYYYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following:					
Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following:					
In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____					
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE THIS DD 254 IS FOR SOLICITATION PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE PROVIDED UPON CONTRACT AWARD.		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip)</i>		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip)</i>		
8. ACTUAL PERFORMANCE					
a. LOCATION		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip)</i>		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT					
NEXT GENERATION ENTERPRISE NETWORK (NGEN) TRANSPORT AND ENTERPRISE SERVICES CONTRACT.					
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X
b. RESTRICTED DATA		X		b. RECEIVE CLASSIFIED DOCUMENTS ONLY	X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X
d. FORMERLY RESTRICTED DATA			X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X
e. INTELLIGENCE INFORMATION:				e. PERFORM SERVICES ONLY	X
(1) Sensitive Compartmented Information (SCI)			X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X
(2) Non-SCI		X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X
f. SPECIAL ACCESS INFORMATION			X	h. REQUIRE A COMSEC ACCOUNT	X
g. NATO INFORMATION		X		i. HAVE TEMPEST REQUIREMENTS	X
h. FOREIGN GOVERNMENT INFORMATION			X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X
i. LIMITED DISSEMINATION INFORMATION			X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X
j. FOR OFFICIAL USE ONLY INFORMATION		X		l. OTHER <i>(Specify)</i>	X
k. OTHER <i>(Specify)</i> NNPI		X		SIPRNET	

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (Specify):

COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND (SPAWARSYSCOM), CODE 8.5.1, 4301 PACIFIC HIGHWAY, SAN DIEGO CA 92110-3127
RELEASE OF COMSEC MATERIAL IS NOT AUTHORIZED.
RELEASE OF RESTRICTED DATA IS NOT AUTHORIZED.
RELEASE OF INTELLIGENCE INFORMATION IS NOT AUTHORIZED.
RELEASE OF NATO MATERIAL IS NOT AUTHORIZED.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
 * In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract, and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

CLASSIFICATION GUIDES:

OPNAVINST 5513.10C, 10-12; NAVAL COMPUTER SECURITY (FORMERLY SECURITY, ADP)

ACCESS REQUIREMENTS:

THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) IS CAROL APPLGARTH, PEO-EIS, 202-433-7391
 THE ALTERNATE COR IS WILLIE JORDAN, PEO EIS, 202-433-7199
 THE CONTRACTING OFFICER IS CDR JOHN WINDOM, SPAWAR 2.1.5, 202-433-7317

10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF THE PEO EIS TECHNICAL CODE. ACCESS TO ANY COMSEC INFORMATION REQUIRES SPECIAL BRIEFINGS AT THE CONTRACTOR FACILITY. ACCESS TO CLASSIFIED COMSEC INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL. USE OF COMSEC INFORMATION IS GOVERNED BY THE NSA INDUSTRIAL COMSEC MANUAL, NSA/CSS POLICY MANUAL 3-16.

ALL CLASSIFIED INFORMATION MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER 13526, CLASSIFIED NATIONAL SECURITY INFORMATION, OF 29 DECEMBER 2009. YOUR DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY REPRESENTATIVE (IS REP) SHOULD BE CONTACTED FOR ASSISTANCE.

COPIES OF ALL SUBCONTRACT DD FORM 254S MUST BE PROVIDED TO THE DISTRIBUTION LISTED IN BLOCK 17.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. YES NO
 (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement that identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

SPECIFIC ON-SITE SECURITY REQUIREMENTS ARE ATTACHED. FOR AUTHORIZED VISITS TO OTHER U.S. GOVERNMENT ACTIVITIES, THE CONTRACTOR MUST COMPLY WITH ALL ONSITE SECURITY REQUIREMENTS OF THE HOST COMMAND. INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS ARE ATTACHED AND **MUST** BE PASSED TO SUBCONTRACTORS:
 FOR OFFICIAL USE ONLY (FOUO) GUIDANCE ATTACHED.
 OPERATIONS SECURITY (OPSEC) REQUIREMENTS ATTACHED AND **MUST** BE PASSED TO SUBCONTRACTORS.
 INTELLIGENCE REQUIREMENTS ARE ATTACHED.
 NNPI REQUIREMENTS ARE ATTACHED.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. YES NO
 (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL ALICIA RHAMY ALICIA.RHAMY@NAVY.MIL	b. TITLE SECURITY'S CONTRACTING OFFICER'S REPRESENTATIVE (COR)	c. TELEPHONE (Include Area Code) (619) 221-7638
---	---	--

d. ADDRESS (Include Zip Code)
 COMMANDER
 SPACE AND NAVAL WARFARE SYSTEMS COMMAND
 4301 PACIFIC HIGHWAY
 SAN DIEGO, CA 92110-3127

17. REQUIRED DISTRIBUTION
 a. CONTRACTOR
 b. SUBCONTRACTOR
 c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
 d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
 e. ADMINISTRATIVE CONTRACTING OFFICER SPAWAR CODE 2.1.5 (WINDOM)
 f. OTHERS AS NECESSARY SPAWAR CODE 8.3.3, PEO EIS (APPLGARTH/JORDAN)

e. SIGNATURE

 20120501

10.B ACCESS TO RESTRICTED DATA REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL. PERMISSION OF THE PEO EIS TECHNICAL CODE IS REQUIRED PRIOR TO SUBCONTRACTING.

10.E(2) PRIOR APPROVAL OF THE PEO EIS TECHNICAL CODE IS REQUIRED FOR SUBCONTRACTING.

10.G CONTRACTOR IS REQUIRED TO BE BRIEFED AND GRANTED ACCESS TO NORTH ATLANTIC TREATY ORGANIZATION (NATO) FOR THE SOLE PURPOSE OF ACCESSING SIPRNET. THIS ACCESS MUST BE NOTED IN JPAS IAW CNO LTR 5510 SER N09N2/8U223003 OF 20 JAN 2008. FOR THE DURATION OF ENDURING FREEDOM CONTRACTOR PERSONNEL WITH ESTABLISHED NEED-TO-KNOW, WHO HAVE BEEN ISSUED AN INTERIM SECURITY CLEARANCE FOR ACCESS TO U.S. CLASSIFIED INFORMATION, ARE ELIGIBLE FOR ACCESS TO NATO INFORMATION OF AN EQUIVALENT LEVEL CLASSIFICATION. THE SPECIAL BRIEFING IS PROVIDED BY THE CONTRACTING COMPANY'S FACILITY SECURITY OFFICER.

10.K ACCESS TO NNPI MATERIAL IS AUTHORIZED.

11.D APPROXIMATELY 25 GSA APPROVED CONTAINERS FOR STORAGE WILL BE REQUIRED ON THIS CONTRACT.

11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS LOCATIONS: TRAVEL REQUIREMENTS ARE DICTATED BY PROGRAM REQUIREMENTS AND CANNOT BE PREDICTED IN ADVANCE. IF OVERSEAS TRAVEL IS REQUIRED, PRIOR APPROVAL FROM THE PROGRAM OFFICE/COR/TR IS REQUIRED AND SPECIFIC SITE WILL BE APPROVED AT THAT TIME. ANTI-TERRORISM/FORCE PROTECTION BRIEFINGS ARE REQUIRED FOR ALL PERSONNEL (MILITARY, DOD CIVILIAN, AND CONTRACTOR) PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL. THE BRIEFING IS AVAILABLE AT [HTTPS://ATLEVEL1.DTIC.MIL/AT/](https://atlevel1.dtic.mil/at/), IF UNABLE TO ACCESS THE WEBSITE CONTACT [SSC_FORTRAV@NAVY.MIL](mailto:ssc_fortrav@navy.mil). SERE 100 LEVEL B CODE OF CONDUCT TRAINING IS ALSO REQUIRED PRIOR TO OCONUS TRAVEL FOR ALL PERSONNEL. SERE 100 TRAINING CAN BE ACCESSED AT [HTTPS://WWW.NKO.NAVY.MIL/PORTAL/HOME/](https://wwwa.nko.navy.mil/portal/home/). PERSONNEL UTILIZING THIS SITE MUST HAVE A CAC CARD. A SERE 100 TRAINING DISK CAN BE BORROWED AT THE SSC PACIFIC POINT LOMA OFFICE OR OLD TOWN CAMPUS OFFICE. SPECIALIZED TRAINING FOR SPECIFIC LOCATIONS, SUCH AS SOUTHCOM HUMAN RIGHTS, OR U.S. FORCES KOREA ENTRY TRAINING, MAY ALSO BE REQUIRED, SSC PACIFIC SECURITY PERSONNEL WILL INFORM YOU IF THERE ARE ADDITIONAL TRAINING REQUIREMENTS.

11.L THE CONTRACTOR IS AUTHORIZED THE USE OF SIPRNET FOR THIS EFFORT.

NO FURTHER ENTRIES ON THIS PAGE.

REQUIREMENTS FOR PROTECTION OF NAVAL NUCLEAR PROPULSION INFORMATION

1. General Protections

- 1.1. Naval Nuclear Propulsion Information (NNPI) shall be safeguarded at all times on the NMCI. Safeguards shall be applied so that such information is accessed only by authorized individuals, is used only for its intended purpose, retains its content integrity, and is marked, handled, and disposed of properly, as required by NAVSEAINST 5511.32C (current series).
- 1.2. The safeguarding of NNPI and NMCI resources (against sabotage, tampering, denial of services, espionage, fraud, misappropriation, misuses, or release to unauthorized persons) shall be accomplished through the continuous employment of safeguards consisting of administrative, procedural, physical and/or environmental, personnel, communications security, emanations security, and computer security (i.e. hardware, firmware and software), as required. The mix of safeguards selected shall achieve the requisite level of security or protection.
- 1.3. 5511.32C (current series) contains security requirements to properly protect NNPI. Specific controls may not be offered by NMCI. Users processing NNPI are responsible for protecting the data in accordance with 5511.32C and must either work with the NMCI program office to request NMCI to develop the needed controls or design an alternative approach to protecting NNPI and obtain NAVSEA 08 approval.
- 1.4. Some specific requirements in 5511.32C (current series) have been modified for use on NMCI systems based on the overall security posture of NMCI and are specifically called out in the following sections: (5.3.1, 5.4.1, 5.5.1, 7.5.3.1, 7.5.3.3, and 9.1.).
- 1.5. NAVSEA 08 approval of overall security approach to include annual assessments, and approval of systems processing NNPI will be handled through Naval Reactors concurrence during the normal Navy certification and accreditation process.

2. Definitions

- 2.1. Naval Nuclear Propulsion Information (NNPI) – Per NAVSEAINST 5511.32C (current series): all information, classified or unclassified, 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 may be unclassified (U-NNPI) or classified (C-NNPI). For this document, statements concerning “NNPI” shall apply equally and separately to both U-NNPI and C-NNPI.
- 2.2. U-NNPI Community of Interest (COI) – The group of unclassified NMCI users who are U.S. citizens and have a need to know U-NNPI.
- 2.3. C-NNPI COI – The group of SECRET NMCI users who are U.S. citizens, have final Government clearances of SECRET or higher, and have a need to know C-NNPI.
- 2.4. NNPI Community of Interest Officer (NNPI COIO) – Any activity that routinely deals with NNPI on NMCI shall designate an individual familiar with NNPI protection requirements as the NNPI COIO. Each activity shall ensure that the NNPI COIO is technically qualified, or that a technically qualified person shall be available for their consultation. The NNPI COIO's primary responsibility shall be to ensure that only site personnel with a need-to-know are granted and allowed to retain access to the NNPI community of interest on the NMCI. If there is an NNPI Control Officer as defined by NAVSEAINST 5511.32C (current series), that individual shall be or shall designate the site NNPI COIO.
- 2.5. NNPI Workspace – A physical area that is designated by the Government as a location for hardware that may process NNPI. An area shall be designated an NNPI workspace only if there are physical security measures in place to prevent unrestricted access to the area by non-U.S. citizens.
- 2.6. U-NNPI Hardware – Unclassified NMCI hardware (e.g., seats, servers, backup tapes, routers and printers) that is designated for storage or transmission of U-NNPI.
- 2.7. C-NNPI Hardware – SECRET NMCI hardware (e.g., seats, servers, backup tapes, routers and printers) that is designated for storage or transmission of C-NNPI.

3. The Contractor is responsible for the confidentiality, integrity, authenticity, identification, access control, non-repudiation, survivability, and availability of Naval Nuclear Propulsion Information (NNPI) contained on the NMCI. The Contractor is not responsible for designating data as NNPI or disclosure of NNPI by authorized NNPI COI users.
4. The Contractor shall implement hardware and system configuration measures for protection of NNPI in such a manner that NMCI users may not compromise them.
5. Hardware
 - 5.1. The Contractor shall assume that all NNPI hardware actually stores NNPI.
 - 5.2. The Contractor shall store information identified by the Government as NNPI only on NNPI hardware.
 - 5.3. Labeling
 - 5.3.1. The Contractor shall label all user-accessible U-NNPI hardware as such. This includes seats (desktop and portable), printers, and wall plugs. The labeling should indicate either "Approved up to Unclassified NNPI" or "NOFORN". Classified NMCI seats used for processing C-NNPI shall have an indicator such as a label or title bar on the monitor while the seat is in use for C-NNPI that indicate the seat is: "Approved for Processing up to Secret NNPI"
 - 5.3.2. The Contractor shall ensure that notices are posted at the entries to server farms, identifying the potential presence of NNPI.
 - 5.3.3. It is not necessary to label equipment that transmits encrypted NNPI.
 - 5.3.4. These requirements satisfy the requirement of NAVSEAINST 5511.32C (current series) that ADP equipment will be marked to identify the highest level of information authorized.
 - 5.4. An NMCI seat designated as NNPI hardware shall not have a foreign national seat configuration (as described in the NMCI SSAA, Appendix P, Security Concept of Operations).
 - 5.4.1. NNPI hardware configuration will comply with the NMCI SSAA Appendix P, Security Concept of Operations, as approved by NNWC.
 - 5.5. NNPI hardware shall be located in a designated NNPI workspace. If non-U.S. citizen access to a NNPI workspace is required, the foreign national shall be escorted by a U.S. citizen, to prevent "unauthorized access to" of any NNPI (per NAVSEAINST 5511.32C) (current series).
 - 5.5.1. Remote access to U-NNPI by a NNWC accredited method such as BuRAS can be obtained from outside a designated NNPI workspace.
6. Communities of interest
 - 6.1. There shall be a community of interest (COI) of users of U-NNPI on the unclassified NMCI.
 - 6.1.1. Users in the U-NNPI COI shall be limited to U.S. citizens. The NNPI COIO will provide a list of authorized COI users to the Contractor.
 - 6.1.2. Users in the U-NNPI COI shall be limited to those unclassified NMCI users with a need to access U-NNPI, as determined by the site NNPI COIO.
 - 6.1.3. Users in the U-NNPI COI shall be identifiable in the unclassified NMCI global address list.
 - 6.2. There shall be a COI of users of C-NNPI on the SECRET NMCI.
 - 6.2.1. Users in the C-NNPI COI shall be limited to U.S. citizens. The NNPI COIO will provide a list of authorized COI users to the Contractor.
 - 6.2.2. Users in the C-NNPI COI shall be limited to those SECRET NMCI users with a need to access C-NNPI, as determined by the site NNPI COIO.
 - 6.2.3. Users in the C-NNPI COI shall be limited to those with final Government clearances of SECRET or higher.
 - 6.2.4. Users in the C-NNPI COI shall be identifiable in the SECRET NMCI global address list.
7. Access to NNPI
 - 7.1. NNPI data on NMCI shall be accessible only by a member of the NNPI COI logged on an NMCI seat that is designated for NNPI use. NNPI data includes data stored on shared file servers; web pages; applications; e-mail; temporary files; swap files; and memory files.
 - 7.2. A member of the NNPI COI shall be able to log on to an NMCI seat designated for NNPI, shall be able to access NNPI, and shall be able to access other data and services on NMCI.
 - 7.2.1. When a member of the U-NNPI COI logs on to an unclassified NMCI seat that is U-NNPI hardware, there shall be a splash screen displayed:

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

U-NNPI is not for release to foreign nationals and has special handling requirements (NOFORN). U-NNPI is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the Chief of Naval Operations (Director, Naval Nuclear Propulsion, DIR NNP (NOON)). 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."

- 7.2.2. When a member of the C-NNPI COI logs on to a SECRET NMCI seat that is C-NNPI hardware, there shall be a splash screen displayed:

"You are approved to process up to and including SECRET naval nuclear propulsion information (NNPI) on the NMCI.

NNPI is not for release to foreign nationals and has special handling requirements (NOFORN). NNPI is subject to special export controls and each transmittal to foreign governments or foreign nationals may be made only with prior approval of the Chief of Naval Operations (Director, Naval Nuclear Propulsion, DIR NNP (NOON)). 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."

- 7.2.3. Splash screens shall require user action to dismiss.

- 7.3. Any NMCI user who is not a member of the U-NNPI COI shall not be able to log on to an NMCI seat that is designated for U-NNPI use, shall not be able to access U-NNPI, and shall not be able to access other data and services on NMCI from U-NNPI hardware.

- 7.4. A member of the U-NNPI COI shall be able to log on to an NMCI seat not designated for U-NNPI use, shall not be able to access U-NNPI, and shall be able to access other data and services on NMCI.

7.5. Content

- 7.5.1. The Contractor shall develop and maintain information system architecture and procedures, by which the Government will mark, store, retrieve, transmit and output (e.g., hard copy or removable media) NNPI data in the NMCI. Government user failure to follow these procedures is outside the scope of Contractor control.

- 7.5.2. All "generic" NMCI data and services shall be accessible from NMCI seats designated to process NNPI.

7.5.3. E-mail

- 7.5.3.1. Members of the U-NNPI COI shall not be permitted to provide read or proxy rights to their e-mail accounts to non-members of the U-NNPI COI.
- 7.5.3.2. Members of the NNPI COI shall not be permitted to access e-mail marked to contain NNPI from a remote access NMCI seat unless that seat is designated for NNPI use and is connected to the NMCI using an approved connection method for accessing NNPI remotely.
- 7.5.3.3. E-mail filtering on outbound traffic, retention of messages and backup and file storage must be in accordance with Navy policy as specified in the NMCI SSAA.

8. Transmission

8.1. Onsite transmission

- 8.1.1. NNPI transmitted within an NNPI workspace does not require encryption provided the originating point, transmission lines, and ending point are capable of being visually monitored or protected in a manner that will allow detection of tampering.
- 8.1.2. C-NNPI transmission onsite must be in accordance with the requirements of NSTISSI No. 7003, Protective Distribution Systems (PDS), dated 13 December 1996.

- 8.2. Any NNPI transmitted offsite must be encrypted.

- 8.3. Encryption
 - 8.3.1. Encryption of U-NNPI must be accomplished by a method that meets FIPS 140-1 or FIPS 140-2 requirements.
 - 8.3.2. Encryption of C-NNPI must be accomplished by a method that meets NSA Type 1 requirements.
- 9. Auditing - As a part of ongoing collection of security data, the Contractor shall continually monitor for suspicious activity associated with NNPI in accordance with Attachment 4 to the basic contract. NAVSEA 08 will provide separately criteria for suspicious activity associated with NNPI.
 - 9.1. Auditing requirements for approved remote access connections to U-NNPI will comply with procedures included in the SSAA and approved with an IATO/ATO for this service as authorized by NNWC.
- 10. Incident Response - If NNPI is stored on non-NNPI hardware, that hardware shall be immediately made inaccessible to anyone on the NMCI, except those involved in evaluating the incident. The hardware shall not be returned to service without the agreement of the NNPI COIO.
- 11. The Contractor shall document NMCI architecture, procedures, and test plans and results for protection of NNPI in appendices to the NMCI System Security Authorization Agreement (SSAA). One appendix shall address U-NNPI on the unclassified NMCI; the other appendix shall address C-NNPI on the SECRET NMCI.

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS

The U.S. Government conducts trustworthiness investigations of personnel who are assigned to positions that directly or indirectly affect the operation of unclassified IT resources and systems that process Department of Defense (DoD) information, to include For Official Use Only (FOUO) and other controlled unclassified information.

The United States Office of Personnel Management (OPM), Federal Investigations Processing Center (FIPC) process all requests for U.S. Government trustworthiness investigations. Requirements for these investigations are outlined in paragraph C3.6.15 and Appendix 10 of DoD 5200.2-R, available at <http://www.dtic.mil/whs/directives/corres/html/52002r.htm>. Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories listed below. The contractor shall include all of these requirements in any subcontracts involving IT support. (Note: Terminology used in DoD 5200.2R references "ADP" vice "IT". For purposes of this requirement, the terms ADP and IT are synonymous.)

The Program Manager (PM), Contracting Officer's Representative (COR) or Technical Representative (TR) shall determine if they or the contractor shall assign the IT Position category to contractor personnel and inform the contractor of their determination. If it is decided the contractor shall make the assignment, the PM, COR, or TR must concur with the designation.

DoDD Directive 8500.1, Subject: Information Assurance (IA), paragraph 4.8 states "Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2R for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R (reference (o))." DoD 5200.2R and DoDD 5200.2 require all persons assigned to sensitive positions or assigned to sensitive duties be U.S. citizens. All persons assigned to IT-I and IT-II positions, as well as all persons with access to controlled unclassified information (without regard to degree of IT access) or performing other duties that are considered "sensitive" as defined in DoDD 5200.2 and DoD 5200.2R must be U.S. citizens. Furthermore, access by non-U.S. citizens to unclassified export controlled data will only be granted to persons pursuant to the export control laws of the U.S. The categories of controlled unclassified information are contained in Appendix 3 of DoD 5200.1R. These same restrictions apply to "Representatives of a Foreign Interest" as defined by DoD 5220.22-M (National Industrial Security Program Operating Manual, NISPOM).

Criteria For Designating Positions:

IT-I Position (Privileged)

- Responsibility or the development and administration of Government computer security programs, and including direction and control of risk analysis and/or threat assessment.
- Significant involvement in life-critical or mission-critical systems.
- Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting grave damage or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater, or (2) lesser amounts if the activities of the individual are not subject to technical review by higher authority in the IT-I category to ensure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.
- Other positions as designated by Space and Naval Warfare Systems Command that involve relatively high risk for effecting grave damage or realizing significant personal gain.

Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated

every 5 years by using the Electronic Questionnaire for Investigation Processing (eQIP) web based program (SF86 format).

IT-II Position (Limited Privileged)

Responsibility for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the IT-I category, includes but is not limited to:

- Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
- Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year. Other positions are designated by Space and Naval Warfare Systems Command that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT-I positions. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check with Local Agency Check and Credit Check (NACLIC).

IT-III Position (Non-Privileged)

- All other positions involving Federal IT activities. Incumbent in this position has non-privileged access to one or more DoD information systems, application, or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudicated NACLIC.

Qualified Cleared Personnel Do **NOT** Require Trustworthiness Investigations:

When background investigations supporting clearance eligibility have been submitted and/or adjudicated to support assignment to sensitive national security positions, a separate NACLIC to support IT access will normally not be required. A determination that an individual is NOT eligible for assignment to a position of trust will also result in the removal of eligibility for security clearance. Likewise, a determination that an individual is NOT eligible for a security clearance will result in the denial of eligibility for a position of trust.

The Facility Security Officer (FSO) must verify employee's security clearance eligibility in the Joint Personnel Adjudication System (JPAS) before instructing the individual to complete and submit the Public Trust Position Application, Standard Form (SF)85P, for trustworthiness determination.

Procedures for submitting U.S. Government Trustworthiness Investigations:

Only hard copy SF85Ps are acceptable by OPM-FIPC. The contractor will ensure personnel complete either the hard copy SF 85P or the online—fillable form of the SF85P. The SF85P is available from OPM at <http://www.opm.gov>.

The SF85P - request package, shall include:

- A hard copy of the SF85P;
- All pertinent signed release forms;
- SF87 or FD258 Fingerprint Card or electronic fingerprint transmission

The company's Facility Security Officer (FSO) is responsible for completing the following items located on the top portion of the SF85P: 1) Clearly indicate for item "A" if the Trustworthiness Investigation is for an 08B (IT-II position) or an 02B (IT-III position); 2) item "B" Extra Coverage enter R, this will allow the Government to request for the finger print data quickly so that a Common Access Card (CAC) can be processed if needed. 3) item "C" is for the Sensitivity/Risk Level enter either 1 (low risk positions), 5 (moderate risk positions), or 6 (high risk positions); 4) item "D" for Computer/ADP (IT) enter I, II, or III; 5) item "E" for the Nature of Action Code enter CON; 6) item "I" must contain the name of the position and the contract number; 7) item "J"

SON enter 4219; 8) item "K" place and X by "None"; 9) item "L" SOI enter NV00; 10) item "M" place and X by "None"; 11) item "N" type DOD-NAVY; 12) item "O" Accounting-Data and/or Agency Case Number enter contracting facility's Cage Code; and 13) item "P" Company representatives/FSO are NOT to sign the SF85P, you must leave this blank.

The company shall review the SF85P for completeness and use SECNAV M-5510.30, Appendix G available at <https://doni.daps.dla.mil/secnavmanuals.aspx> to determine if any adverse information is present. Additional guidance for requesting investigations from OPM is found at <http://www.opm.gov>. Completed SF85P packages will be mailed "in care of" to: Commanding Officer, Space and Naval Warfare Systems Center Pacific, Code 83310 (SF85P), 53560 Hull Street, San Diego, CA 92152-5001. Note: All forms must be signed by the individual within 60 days of the date of submission. Submitted forms, which are not received within these 60 days, will be delayed or returned. If no change has occurred, forms must be re-dated and initialed by the Subject/employee. If the SF85P is submitted with missing information or adverse information is found, the form(s) will be returned to the company/FSO to revised and resubmit.

The Office of the Chief Naval Operations has provided the following guidance in their letter Ser N09N2/8U223257 dated 9 October 2008 which states in paragraph 2 that the "contractor fitness determinations made by the DON CAF will be maintained in the Joint Personnel Adjudication System (JPAS). Favorable fitness determinations will support public trust positions only and not national security eligibility. If no issues are discovered, according to respective guidelines a "Favorable Determination" will be populated in JPAS and will be reciprocal within DoN. If issues are discovered, the DoN CAF will place a "No Determination Made" in the JPAS and forward the investigation to the submitting office for the commander's final determination."

For Trustworthiness Investigations that have been returned to Space and Naval Warfare Systems Center Pacific Security Office with a "No Determination Made" decision, your company will be notified in writing. If an individual received a negative trustworthiness determination, they will be immediately removed from their position of trust, the contractor will follow the same employee termination processing above, and they will replace any individual who has received a negative trustworthiness determination.

If you require additional assistance for SF85P or related concerns, you may send email to SPAWARSSYSCEN PAC at SSC_PAC_SF85P@NAVY.MIL.

SPECIFIC ON-SITE SECURITY REQUIREMENTS

I. GENERAL.

- a. **Contractor Performance.** In performance of this Contract the following security services and procedures are incorporated as an attachment to the DD 254. The Contractor will conform to the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program, Operating Manual (NISPOM). When visiting the Program Executive Office, Enterprise Information Systems (PEO EIS) at Old Town Campus (OTC) the Contractor will comply with the security directives used regarding the protection of classified and controlled unclassified information, SECNAVINST 5510.36 (series), SECNAVINST 5510.30 (series), and SPAWARINST 5510.1. Both of the SECNAV Instructions are available online at <http://neds.nebt.daps.mil/directives/table52.html>. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location from PEO EIS, the security provisions of the NISPOM will be followed within this cleared facility.
- b. **Security Supervision.** Space and Naval Warfare Systems Center Pacific will exercise security supervision over all contractors visiting PEO EIS and will provide security support to the Contractor as noted below. The Contractor will identify, in writing to Security's COR, an on-site Point of Contact to interface with Security's COR.

II. HANDLING CLASSIFIED MATERIAL OR INFORMATION.

- a. **Control and Safeguarding.** Contractor personnel located at PEO EIS are responsible for the control and safeguarding of all classified material in their possession. All contractor personnel will be briefed by their FSO on their individual responsibilities to safeguard classified material. In addition, all contractor personnel are invited to attend SPAWARSYSCEN Pacific conducted Security Briefings, available at this time by appointment only. In the event of possible or actual loss or compromise of classified material, the on-site Contractor will immediately report the incident to SPAWARSYSCEN Pacific's Code 83310, telephone (619) 553-3005, as well as the Contractor's FSO. A Code 83310 representative will investigate the circumstances, determine culpability where possible, and report results of the inquiry to the FSO and the Cognizant DSS Field Office. On-site contractor personnel will promptly correct any deficient security conditions identified by a SPAWARSYSCEN Pacific Security representative.
- b. **Storage.**
 1. Classified material may be stored in containers authorized by SPAWARSYSCEN Pacific's Physical Security Branch, Code 83320 for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board PEO EIS with Code 83320's written permission. Areas located within cleared contractor facilities on board PEO EIS will be approved by DSS.
 2. The use of Open Storage areas must be pre-approved in writing by Code 83320 for the open storage, or processing, of classified material. Specific supplemental security controls for open storage areas, when required, will be provided by SPAWARSYSCEN Pacific, Code 83320.
- c. **Transmission of Classified Material.**
 1. All classified material transmitted by mail for use by long term visitors will be addressed as follows:
 - (a) TOP SECRET, Non-Sensitive Compartmented Information (non-SCI) material using the Defense Courier Service: SPAWARSYSCEN-PACIFIC: 271582-SN00, SPAWARSYSCEN PACIFIC.
 - (b) CONFIDENTIAL and SECRET material transmitted by FedEx will be addressed to COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC, ATTN RECEIVING OFFICER CODE 43150, 4297 PACIFIC HIGHWAY, SAN DIEGO, CA 92110.

(c) CONFIDENTIAL and SECRET material transmitted by USPS Registered and Express mail will be addressed to COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC, 53560 HULL STREET, SAN DIEGO CA 92152-5001. The inner envelope will be addressed to the attention of the Contracting Officer's Representative (COR) or applicable Technical Representative (TR) for this contract, to include their code number.

2. All SECRET material hand carried to PEO EIS by contractor personnel must be delivered to the Classified Material Control Center (CMCC), Code 83430, building 33, room 1305, for processing.
3. All CONFIDENTIAL material hand carried to PEO EIS by contractor personnel that is intended to remain at PEO EIS shall be provided to the designated recipient or proper cleared PEO EIS & SPACE employee.
4. All PEO EIS classified material transmitted by contractor personnel from PEO EIS will be sent via the PEO EIS Technical COR or TR for this contract.
5. The sole exception to the above is items categorized as a Data Deliverable. All contract Data Deliverables will be sent directly to the Technical COR or TR and a notification of deliverables without attachments will be sent to the cognizant PCO, unless otherwise stated in the contract.

III. INFORMATION ASSURANCE (IA) Security. Contractors using Information Technology (IT), networks, or computer resources to process classified, sensitive unclassified and/or unclassified information will comply with the provisions of SECNAVINST 5239.3 (series) and local policies and procedures. Contractor personnel must ensure that systems they use at PEO EIS have been granted a formal letter of approval to operate by contacting their Information Assurance Office.

IV. VISITOR CONTROL PROCEDURES.

Title 18 USC 701 provides for criminal sanctions including fine or imprisonment for anyone in possession of a badge who is not entitled to have possession. Sec. 701. Official badges, identification cards, other insignia. Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both.

- a. Contractor personnel assigned to PEO EIS will be considered long-term visitors for the purpose of this contract.
- c. CONTRACTORS WHO HAVE BEEN AWARDED A CLASSIFIED ACCESS CONTRACT MUST SUBMIT VISIT REQUESTS USING ONLY THE JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS). ALL GOVERNMENT ACTIVITIES HAVE BEEN DIRECTED TO USE JPAS WHEN TRANSMITTING OR RECEIVING VISIT REQUESTS. CONTRACTORS WHO WORK ON CLASSIFIED ACCESS CONTRACTS ARE REQUIRED TO HAVE ESTABLISHED AN ACCOUNT THROUGH JPAS FOR THEIR FACILITY. THIS DATABASE CONTAINS ALL U.S. CITIZENS WHO HAVE RECEIVED A CLEARANCE OF CONFIDENTIAL, SECRET, AND/OR TOP SECRET. THE VISIT REQUEST CAN BE SUBMITTED FOR ONE YEAR. WHEN SUBMITTING VISIT REQUESTS TO PEO EIS AT OLD TOWN CAMPUS USE THE SECURITY MANAGEMENT OFFICE (SMO) NUMBER (660015). THIS INFORMATION IS PROVIDED IN ACCORDANCE WITH GUIDANCE PROVIDED TO CONTRACTORS VIA THE DEFENSE SECURITY SERVICE (DSS) WEBSITE
[HTTPS://WWW.DSS.MIL/PORTAL/SHOWBINARY/BEA%20REPOSITORY/NEW_DSS_INTERNET/ABOUT_DSS/PRESS_ROOM/JPAS_PROCEDURES_FINAL.PDF](https://www.dss.mil/portal/showbinary/bea%20repository/new_dss_internet/about_dss/p ress_room/jpas_procedures_final.pdf) (DSS GUIDANCE DATED 24 APRIL 2007, SUBJECT: PROCEDURES GOVERNING THE USE OF JPAS BY CLEARED CONTRACTORS)

- d. For visitors to receive a SPAWAR Systems Center Pacific issued badge their Government point of contact must approve their visit request and the visitor must present government issued photo identification.
 - d. Visit requests for long-term visitors must be received at least one week prior to the expected arrival of the visitor to ensure necessary processing of the request.
 - e. Code 83320 will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible PEO EIS Technical COR/TR will request issuance of picture badges to contractor personnel. Identification badges are the property of the U.S. Government, will be worn in plain sight, and used for official business only. Unauthorized use of an SPAWARSYSCEN Pacific badge will be reported to the DSS.
 - f. Prior to the termination of a Contractor employee with a SPAWARSYSCEN Pacific badge or active VAL on file the FSO must:
 - 1. Notify in writing Code 83320, the Technical COR/TR, Security's COR, and the laboratory managers of any laboratories into which the employee had been granted unescorted access of the termination and effective date. In emergencies, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.
 - 2. Immediately confiscate any SPAWARSYSCEN Pacific issued identification badge, (to include Common Access Card (CAC) and OP Form 55 card, if issued), and vehicle decals and return them to Code 83320 no later than five working days after the effective date of the termination.
 - g. Common Access Card (CAC).
 - 1. VAL must be on file, form completed and signed, approved by the contractor's COR, and sent to the Badge and Pass Office, Code 83320.
- V. INSPECTIONS. Code 83310 personnel may conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel will cooperate with Code 83310 representatives during these inspections. A report of the inspection will be forwarded to the Contractor's employing facility, Security's COR and Technical COR/ Technical Representative. The Contractor must be responsive to the Code 83310 representative's findings.
- VI. REPORTS. As required by the NISPOM, Chapter 1, Section 3, contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), the status of an employee's personnel clearance (PCL), the proper safeguarding of classified information, or an indication classified information has been lost or compromised.
- a. The Contractor will ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 8.3.3. If further investigation is warranted it will be conducted by Code 8.3.3. This reporting will include the following:
- 1. The denial, suspension, or revocation of security clearance of any assigned personnel;
 - 2. Any adverse information on an assigned employee's continued suitability for continued access to classified access;
 - 3. Any instance of loss or compromise, or suspected loss or compromise, of classified information;
 - 4. Actual, probable or possible espionage, sabotage, or subversive information; or
 - 5. Any other circumstances of a security nature that would affect the contractor's operation on board

SPAWARSYSCOM.

- b. In addition to the NISPOM reporting requirements, any conviction and/or violation of the Foreign Corrupt Practices Act, or any other violation of the International Traffic in Arms Regulations (ITAR) shall immediately be reported to the Designated Disclosure Authority (DDA), COR/TR/PM and Contracting Officer.

VII. PHYSICAL SECURITY.

- a. SPAWARSYSCEN Pacific will provide appropriate response to emergencies occurring onboard this Command. The Contractor will comply with all emergency rules and procedures established for SPAWARSYSCEN Pacific.
- b. A roving Contract Security Guard patrol will be provided by SPAWARSYSCEN Pacific. Such coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Specific questions or concerns should be addressed to Code 83320.
- c. All personnel aboard SPAWARSYSCEN Pacific property are subject to random inspections of their vehicles and personal items. Consent to these inspections is given when personnel accept either a badge or a vehicle pass/decal permitting entrance to this command.
- d. Information about parking restrictions may be found on the Security web site at <https://iweb.spawar.navy.mil/services/security/html/Parking.html>.

Contractors must comply with installation access control procedures. Any Contractor who repeatedly violates access control requirements will be issued an Apparent Security Violation (ASV). After the ASV has been investigated, a letter will be forwarded to the contracting facility's Security Officer via the Center's Contracting Officer for resolution.

VIII. PROGRAM OFFICE/TECHNICAL REPRESENTATIVE'S RESPONSIBILITIES.

- a. Review requests by cleared contractors for retention of classified information beyond a two-year period and advise the contractor of disposition instructions and/or submit a Final DD 254 to Security's COR.
- b. In conjunction with the appropriate transportation element, coordinates a suitable method of shipment for classified material when required.
- c. Certify and approve Registration For Scientific and Technical Information Services requests (DD 1540) (DTIC).
- d. Ensure timely notice of contract award is given to host commands when contractor performance is required at other locations.
- e. Certify need-to-know on visit requests and conference registration forms.

IX. SPECIAL CONSIDERATIONS FOR ON-SITE CLEARED FACILITIES.

Any cleared contractor facility on board PEO EIS will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional PEO EIS contracts may be performed in this cleared facility, but only on a case-by-case basis. The COR, Security's COR, and Contracting Officer must all be in agreement that this particular arrangement best suits the needs of the Government. At the end of this contract the on-site facility must be vacated, with proper written notification being submitted to the DSS and Security's COR.

X. ITEMS PROHIBITED ABOARD PEO EIS AND SPAWAR.

The following items are prohibited within any PEO EIS and SPAWAR controlled areas, with the exception of personnel authorized to possess weapons in the performance of required duties. Also, note exceptions for alcohol possession and consumption on board PEO EIS or SPAWAR property.

WEAPONS

1. Ammunition
2. Fireworks
3. Molotov Cocktail
4. Pipe Bomb
5. Black Jack
6. Slingshots
7. Billy/Sand Club
8. Nunchakus
9. Sand Bag: Partially filled with sand and swung like a mace
10. Metal (Brass) Knuckle
11. Dirk or Dagger
12. Switch Blade or Butterfly Knife
13. Knife with a blade (cutting edge) longer than 4 inches
14. Razor with Unguarded blade.
15. Pipe, Bar or Mallet to be used as a club.
16. Compressed Air or Spring Fired Pellet/BB gun
17. Tear Gas/Pepper Spray Weapon
18. Pistol, Revolver, Rifle, Shotgun or any other Firearm
19. Bows, Crossbows or Arrows
20. Bowie Style Hunting Knife
21. Any weapon prohibited by State law
22. Any object similar to the aforementioned items
23. Any offensive or defensive weapons not described above, but likely to cause injury (i.e., Stun Gun, Blow Gun).
24. Any abrasive, caustic, acid, chemical agent or similar substance, with which to inflict property damage or personal injury
25. Combination Tools with Knife Blades Longer Than 4 inches (i.e., Gerber, Leatherman, etc.)

Military personnel aboard PEO EIS and SPAWARSYSCEN Pacific controlled areas not authorized to possess a firearm, as part of prescribed military duties will be apprehended if found in possession. Civilians in unauthorized possession of a firearm will be detained while civilian authorities are notified.

CONTROLLED SUBSTANCES

The unauthorized possession or use of controlled substances defined as marijuana, narcotics, hallucinogens, psychedelics, or other controlled substances included in Schedule I, II, III, IV, or V established by Section 202 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (84 Stat. 1236) is prohibited.

CONTRABAND

Contraband defined as all equipment, products and materials of any kind which are used, intended for use, or designed for use in injecting, ingesting, inhaling, or otherwise introducing into the human body, marijuana or other controlled substances, in violation of law. This includes: hypodermic syringes, needles, and other objects to inject controlled substances in the body or objects to ingest, inhale or otherwise introduce marijuana, cocaine

or hashish oil into the body is prohibited.

ALCOHOL

All PEO EIS, tenant command and other government employees, as well as support contractors and authorized visitors may bring unopened containers of alcohol on board the Center if it remains in their private vehicles except where expressly authorized for an approved event. Alcohol beverages will be consumed only at designated facilities for which written permission by the Commanding Officer is granted.

Personnel desiring to hold a social function and serve alcohol, should send a memo (hard copy) to the Commanding Officer, via the appropriate division head, the Director of Security, and the Public Affairs Officer. The Public Affairs Officer will approve or disapprove the facility use request based on availability and general use policy. If facility use is approved, the Public Affairs Officer will forward the memo to the Commanding Officer for approval/disapproval.

COUNTERFEIT CURRENCY

Counterfeit currency defined as any copy, photo, or other likeness of any U.S. currency, either past or present, not authorized by the U.S. Treasury Department is prohibited.

XI. ESCORTING POLICY.

- a. All personnel within PEO EIS and SPAWARSYSCEN Pacific's fenced perimeters, with the exception of emergency personnel such as fire, ambulance, or hazardous material response personnel responding to an actual emergency, must wear an SPAWARSYSCEN Pacific issued badge. Only U.S. citizens and U.S. Permanent Residents may be escorted under this policy. ALL PEO EIS FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE SPAWAR FOREIGN VISITS COORDINATOR OFFICE, 8335. Contact phone number: (858) 537-8884.
- b. All pictured badged PEO EIS and tenant command employees, as well as those contractors and other government employees who have an "E" on their picture badge may escort visitors wearing a red escort-required badge.

XIII. CELLULAR PHONE USAGE.

- a. Cellular phone use is prohibited in all secure spaces, i.e. Open Storage areas, classified laboratories.
- b. Vehicle operators on DoD installations and operators of Government vehicles shall not use cellular phones, unless the vehicle is safely parked or unless they are using a hands-free device, and are also prohibited from wearing of any other portable headphones, earphones, or other listening devices while operating a motor vehicle.
- c. The use of cellular phones, portable headphones, earphones, or other listening devices while jogging, walking bicycling, or skating on roads and streets on Navy installations is prohibited except for use on designated bicycle and running paths and sidewalks.

XIV. PERSONAL ELECTRONIC MEDIA

The use of personal electronic media (computer laptops, flash (thumb), or other removable drives) is prohibited in team SPAWAR spaces except where explicitly permitted by the COMSPAWARSYSCOM Director of Security, (858) 537-8898. All removable electronic media must be labeled (unclassified, etc.) To the highest classification of data stored, and/or for the classification of the system in which it is used. If classified, any removable electronic media must be tracked and stored appropriate to that level of classification.

CONTRACTOR REQUIREMENTS FOR ACCESS TO INTELLIGENCE INFORMATION

1. Intelligence material and information, either furnished by the user agency or generated under the contract performance, will not be:
 - a. Reproduced without prior approval of the originator of the material. All Intelligence material shall bear a prohibition against reproduction while in your custody; or
 - b. Released to foreign nationals or immigrant aliens who you may employ, regardless of their security clearance or access authorization, except with the specific permission of the Office of Naval Intelligence (ONI-5), via Security's Contracting Officer's Representative (COR); or
 - c. Released to any activity or person of the contractor's organization not directly engaged in providing services under the contract or to another contractor (including subcontractors), government agency, private individual, or organization without prior approval of the originator of the material, and prior approval and certification of need-to-know by the designated project manager/contract sponsor.
2. Intelligence material does not become the property of the contractor and may be withdrawn at any time. Upon expiration of the contract, all intelligence released and any material using data from the Intelligence must be returned to the COR or authorized representative for final disposition. The contractor shall maintain such records as will permit them to furnish, on demand, the names of individuals who have access to Intelligence material in their custody.
3. Access to Intelligence data will only be through cognizant government program managers/project engineers. Independent access is not inferred or intended.
4. Classified Intelligence, even though it bears no control markings, will not be released in any form to foreign nationals or immigrant aliens (including U.S. government employed, utilized, or integrated foreign nationals and immigrant aliens) without permission of the originator.
5. You will maintain records that will permit you to furnish, on demand, the names of individuals who have access to Intelligence material in your custody.
6. Access to Intelligence data requires the adherence to the requirements set forth in DoD 5105.21-M-1, Department of Defense Sensitive Compartmented Information Administrative Security Manual.

FOR OFFICIAL USE ONLY (FOUO) INFORMATION

1. The For Official Use Only (FOUO) marking is assigned to information at the time of its creation. It isn't authorized as a substitute for a security classification marking but is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).
2. Use of FOUO markings doesn't mean that the information can't be released to the public, only that it must be reviewed by PEO EIS 7 Space prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.
3. An UNCLASSIFIED document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the bottom face and interior pages.
4. Classified documents containing FOUO do not require any markings on the face of the document; however, the interior pages containing only FOUO information shall be marked top and bottom center with "FOR OFFICIAL USE ONLY." Mark only unclassified portions containing FOUO with "(FOUO)" immediately before the portion.
5. Any FOUO information released to you by PEO EIS is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTION(S) _____ APPLY.

6. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. DO NOT REMOVE ANY FOUO MARKING WITHOUT WRITTEN AUTHORIZATION FROM PEO EIS OR THE AUTHOR. When the FOUO status is terminated you will be notified.
7. You may disseminate FOUO information to your employees and subcontractors who have a need for the information in connection with this contract.
8. During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items.
9. FOUO information may be transmitted via first-class mail, parcel post, fourth-class mail for bulk shipments only.
10. When no longer needed, FOUO information may be disposed by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash, or recycle, container or in the uncontrolled burn.
11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.
12. Electronic transmission of FOUO information (voice, data, or facsimile) should be by approved secure communications systems whenever practical.
13. To obtain for official use only (FOUO) guidance refer to the DoD Information Security Program Regulation, DoD 5200.1-R, Appendix 3, located at <http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf>.

OPERATIONS SECURITY (OPSEC) REQUIREMENTS

All work is to be performed in accordance with DoD and Navy Operations Security (OPSEC) requirements, per the following applicable documents:

- National Security Decision Directive 298, National Operations Security Program (NSDD) 298
- DOD 5205.02, DOD Operations Security (OPSEC) Program Manual
- OPNAVINST 3432.1, Operations Security
- SPAWARINST 3432.1, Operations Security (OPSEC) Policy

The contractor will accomplish the following minimum requirements in support of the Space and Naval Warfare Systems Command (SPAWARSYSCOM) OPSEC Program:

- The contractor will practice OPSEC and implement OPSEC countermeasures to protect DoD Critical Information. Items of Critical Information are those facts, which individually, or in the aggregate, reveal sensitive details about SPAWARSYSCOM or the contractor's security or operations related to the support or performance of this SOW, and thus require a level of protection from adversarial collection or exploitation not normally afforded to unclassified information.
- Contractor must protect Critical Information and other sensitive unclassified information and activities, especially those activities or information which could compromise classified information or operations, or degrade the planning and execution of military operations performed or supported by the contractor in support of the mission. Protection of Critical Information will include the adherence to and execution of countermeasures which the contractor is notified by or provided by SPAWARSYSCOM, for Critical Information on or related to the SOW.
- Sensitive unclassified information is that information marked FOR OFFICIAL USE ONLY (or FOUO), Privacy Act of 1974, Company Proprietary, and information identified by SPAWARSYSCOM or the SPAWARSYSCOM Security Representative.
- SPAWARSYSCOM has identified the following items as Critical Information that may be related to this SOW:
 - Known or probable vulnerabilities to any U.S. system and their direct support systems.
 - Details of capabilities or limitations of any U.S. system that reveal or could reveal known or probable vulnerabilities of any U.S. system and their direct support systems.
 - Details of information about military operations, missions, and exercises.
 - Details of U.S. systems supporting combat operations (numbers of systems deployed, deployment timelines, locations, effectiveness, unique capabilities, etc.).
 - Operational characteristics for new or modified weapon systems (Probability of Kill, Countermeasures, Survivability, etc.).
 - Required performance characteristics of U.S. systems using leading edge or greater technology (new, modified, or existing).
 - Telemetered or data-linked data or information from which operational characteristics can be inferred or derived.
 - Test or evaluation information pertaining to schedules of events during which Critical Information might be captured. (advance greater than 3 days).
 - Details of Team SPAWAR unique Test or Evaluation capabilities (disclosure of unique capabilities).
 - Existence and/or details of intrusions into or attacks against DoD Networks or Information Systems, including, but not limited to, tactics, techniques and procedures used, network vulnerabilities exploited, and data targeted for exploitation.
 - Network User ID's and Passwords.
 - Counter-IED capabilities and characteristics, including success or failure rates, damage assessments, advancements to existing or new capabilities.
 - Vulnerabilities in Command processes, disclosure of which could allow someone to circumvent security, financial, personnel safety, or operations procedures.

- o Force Protection specific capabilities or response protocols (timelines/equipment/numbers of personnel/training received/etc.).
- o Command leadership and VIP agendas, reservations, plans/routes etc.
- o Detailed facility maps or installation overhead photography (photo with annotation of Command areas or greater resolution than commercially available).
- o Details of COOP, Team SPAWAR emergency evacuation procedures, or emergency recall procedures.
- o Government personnel information that would reveal force structure and readiness (such as recall rosters or deployment lists).
- o Compilations of information that directly disclose Command Critical Information.

The above Critical Information and any that the contractor develops, regardless if in electronic or hardcopy form, must be protected by a minimum of the following countermeasures:

- All emails containing Critical Information must be DoD Public Key Infrastructure (PKI) signed and PKI encrypted when sent.
- Critical Information may not be sent via unclassified fax.
- Critical Information may not be discussed via non-secure phones.
- Critical Information may not be provided to individuals that do not have a need to know it in order to complete their assigned duties.
- Critical Information may not be disposed of in recycle bins or trash containers.
- Critical Information may not be left unattended in uncontrolled areas.
- Critical Information in general should be treated with the same care as FOUO or proprietary information.
- Critical Information must be destroyed in the same manner as FOUO.
- Critical Information must be destroyed at contract termination or returned to the government at the government's discretion.

The contractor shall document items of Critical Information that are applicable to contractor operations involving information on or related to the SOW. Such determinations of Critical Information will be completed using the DoD OPSEC 5 step process as described in National Security Decision Directive (NSDD) 298, "National Operations Security Program".

OPSEC training must be Included as part of the contractors ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the NISPOM. NSDD 298, DoD 5205.02, "DOD Operations Security (OPSEC) Program", and OPNAVINST 3432.1, "Operations Security" should be used to assist in creation or management of training curriculum.

If the contractor cannot resolve an issue concerning OPSEC they will contact the SPAWARSSYSCOM Security Representative (who will consult with the SPAWARSSYSCOM OPSEC Manager).

All above requirements MUST be passed to all Sub-contractors.

Questions pertaining to the SPAWAR OPSEC Program should be directed to Grant Merkel, 619-553-2800, email grant.merkel@navy.mil.