

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)				a. FACILITY CLEARANCE REQUIRED TOP SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED SECRET	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)		
X	a. PRIME CONTRACT NUMBER N00024-00-D-6000	X	a. ORIGINAL (Complete date in all cases)	Date (YYYYMMDD) 20020830	
	b. SUBCONTRACT NUMBER	X	b. REVISED (Supersedes all previous specs)	Revision No. 5	Date (YYYYMMDD) 20020816
	c. SOLICITATION OR OTHER NO.		c. FINAL (Complete Item 5 in all cases)	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 _____ (Preceding Contract Number) 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 identified classified material is authorized for the period of _____					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE ELECTRONIC DATA SYSTEMS CORPORATION 13600 EDS DRIVE A5N-E31 HERNDON, VA 20171-3225		b. CAGE CODE 1U305	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip) DEFENSE SECURITY SERVICE (DSS) NORTHEAST REGION 7010 LITTLE RIVER TURNPIKE, SUITE 310 ANNANDALE, VA 22003-0308		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)		
8. ACTUAL PERFORMANCE					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT					
NAVY MARINE CORPS INTRANET					
10. THIS CONTRACT 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 SECRET		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 (Specify) INFORMATION TECHNOLOGY (IT) (FORMERLY AIS) CLASSIFIED PROCESSING REQUIRED	X
k. OTHER (Specify)			X		
PR NO.:					

PR NO.:

CONTRACT NUMBER: N00024-00-D-6000

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 to the Directorate for Freedom of Information and

DIRECT THROUGH (Specify):

RELEASE OF COMSEC INFORMATION IS NOT AUTHORIZED.

RELEASE OF NATO INFORMATION IS NOT AUTHORIZED.

RELEASE OF RESTRICTED DATA IS NOT AUTHORIZED.

RELEASE OF SCI INFORMATION IS NOT AUTHORIZED.

COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND, CODE 00L, 4301 PACIFIC HIGHWAY, SAN DIEGO CA 92110-3127

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: (GUIDE(S) PROVIDED UNDER SEPARATE COVER BY TECHNICAL REPRESENTATIVE, PMW 164-1)

OPNAVINST S5513.10B, ENCL 12, NAVAL COMPUTER SECURITY (FORMERLY SECURITY, ADP)

NMCI SECURITY REQUIREMENTS, MAY 2000

ACCESS REQUIREMENTS:

10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF COMSPAWARSYSCOM. 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. STU-III TERMINALS INSTALLED AT THE CONTRACTORS'S FACILITIES SHALL BE SUPPORTED BY A COMSEC ACCOUNT. STU-III's IN SCI FACILITIES (SCIFS) REQUIRE CLASS VI CRYPTOGRAPHIC INGNTIONS KEY (CIK).

BLOCK 13 ACCESS CONTINUED ON NEXT PAGE

CONTRACTING OFFICER'S REPRESENTATIVE (COR) FOR GENSER/SCI: MR. JAMES R. BACHRACH, PMW 164-1, (858) 537-8519

SITE CUSTOMER TECHNICAL REPRESENTATIVE (CTR) OR DEPUTY CTR WILL BE RESPONSIBLE FOR AUTHORIZATION OF FORM DD1172 "APPLICATION FOR DOD COMMON ACCESS CARD." THE CTR OR DCTR WILL ALSO PROVIDE ANY LOCALLY REQUIRED SECURITY RELATED AUTHORIZATIONS (E.G., VEHICLE DECALS, SITE BADGES, ETC).

ALL CLASSIFIED INFORMATION MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER 12958-CLASSIFIED NATIONAL SECURITY INFORMATION, OF 17 APRIL 1995. YOUR DEFENSE SECURITY SERVICE (DSS) INDUSTRIAL SECURITY REPRESENTATIVE (IS REP) SHOULD BE CONTACTED FOR ASSISTANCE.

COPIES OF ALL SUBCONTRACT DD FORM 254'S 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. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed)

(SOME SECURITY REQUIREMENTS ARE SITE SPECIFIC - CONTACT CTR/DEPUTY CTR FOR LOCAL SECURITY REQUIREMENTS)

- 1) NNPI SECURITY REQUIREMENTS ATTACHED.
- 2) INFORMATION TECHNOLOGY (IT) PERSONNEL SECURITY PROGRAM REQUIREMENTS ATTACHED AND SHALL BE PROVIDED TO ALL SUB-CONTRACTORS.
- 3) SPECIFIC ON-SITE SECURITY REQUIREMENTS ATTACHED. SCI REQUIREMENTS ATTACHED.
- 4) INTELLIGENCE INFORMATION REQUIREMENTS ATTACHED.
- 5) FOR OFFICIAL USE ONLY (FOUO) INFORMATION ATTACHED.
- 6) CONTRACTOR TEMPEST QUESTIONNAIRE ATTACHED AND MAY BE PASSED TO SUBCONTRACTORS.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (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.)

CSO AND INSPECTION AUTHORITY FOR SCI IS: DIRECTOR, OFFICE OF NAVAL INTELLIGENCE (523), 4251 SUITLAND ROAD, WASHINGTON, DC 20395-5720 TELEPHONE: (301) 669-2060.

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.

WA SPANAL 08-5 8/16/02

a. TYPED NAME OF CERTIFYING OFFICIAL SUSANV@SPAWAR.NAVY.MIL SUSAN M. VILLARREAL	b. TITLE SECURITY CONTRACTING OFFICER'S REPRESENTATIVE (COR)	c. TELEPHONE (Include Area Code) (619) 524-2672
d. ADDRESS (Include Zip Code) COMMANDING OFFICER SPAWAR SYSTEMS CENTER CODE 20351 53560 HULL ST. SAN DIEGO, CA 92152-5001	17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY Code 20351, PMW 164-1	
e. SIGNATURE 20020820 <i>Susan M. Villarreal</i>		

BLOCK 13 ACCESS REQUIREMENTS CONTINUED:

10.B ACCESS TO RESTRICTED DATA--NAVAL NUCLEAR PROPULSION INFORMATION (NNPI) REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL. REFER TO ATTACHMENT (1) FOR FURTHER INSTRUCTIONS.

10.E(1) CSO AND INSPECTION AUTHORITY FOR SCI IS: DIRECTOR, OFFICE OF NAVAL INTELLIGENCE (523), 4251 SUITLAND ROAD, WASHINGTON, DC 20395-5720 TELEPHONE: (301) 669-2060. **ACCESS TO SCI IS LIMITED TO AN U.S. GOVERNMENT SCIF.**

10.E(2) PRIOR APPROVAL OF COMSPAWARSYSCOM IS REQUIRED FOR SUBCONTRACTING. ACCESS TO INTELLIGENCE INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL.

10.G ACCESS TO NATO INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL AND SPECIAL BRIEFINGS. HIGHEST LEVEL IS NATO SECRET.

11.C MAJORITY OF CLASSIFIED WORK/STORAGE DONE AT A GOVT FACILITY AND/OR OTHER APPROVED/CLEARED CONTRACTOR. FACILITY INFORMATION GENERATED IN PERFORMANCE OF THIS DELIVERY ORDER SHALL BE MARKED IN ACCORDANCE WITH E.O. 12958.

11.D RESTRICTED/CLOSED AREAS AND/OR GSA APPROVED SECURITY CONTAINER(S) WILL BE REQUIRED.

11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS LOCATIONS: GUANTANAMO BAY (CUBA), PUERTO RICO, AND ICELAND.

ANTI-TERRORISM/FORCE PROTECTION BRIEFINGS REQUIRED FOR PERSONNEL PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL.

11.G THE CONTRACTOR IS AUTHORIZED THE USE OF DTIC REGARDING CONTRACT RELATED MATTER AND WILL PREPARE AND PROCESS DD FORM 1540 IN ACCORDANCE WITH THE NISPOM, CHAPTER 11, SECTION 2. THE COR WILL CERTIFY NEED-TO-KNOW TO DTIC. CONTRACTOR GENERATED OR GOVERNMENT FURNISHED MATERIAL MAY NOT BE PROVIDED TO THE DEFENSE TECHNICAL INFORMATION CENTER (DTIC), CONTRACT GENERATED TECHNICAL REPORTS WILL BEAR THE STATEMENT NOT RELEASABLE TO THE DEFENSE TECHNICAL INFORMATION CENTER PER DOD INSTRUCTION 5230.24.

11.K THE CONTRACTING OFFICER AUTHORIZES AUTHORIZATION OF A DEFENSE COURIER SERVICE (DCS) ACCOUNT WITH PRIOR VALIDATION.

11.L CLASSIFIED INFORMATION TECHNOLOGY (COMPUTER) PROCESSING (ASHORE) SHALL BE IN ACCORDANCE WITH THE PROVISIONS OF THE NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM), CHAPTER 8, AND MUST BE PERFORMED ON AN ACCREDITED COMPUTER SYSTEMS APPROVED BY DSS. ALL CLASSIFIED IT PROCESSING ABOARD US FLAG OR FOREIGN FLAG VESSELS SHALL BE IN ACCORDANCE WITH SECNAVINST 5510.36 AND SECNAVINST 5239.2. **ALL PERSONNEL REQUIRING ACCESS TO US GOVERNMENT OWNED OR U.S. GOVERNMENT MANAGED INFORMATION TECHNOLOGY (COMPUTER) SYSTEMS MUST BE U.S. CITIZENS OR U.S. NATIONALS.** SEE ATTACHMENT (2) FOR IT PERSONNEL SECURITY REQUIREMENTS. DEFINITION OF U.S. NATIONAL IS FOUND AT (8 USC SEC. 1401), WEB DIRECTORY SITE: US CODES UNDER TITLE 8, SECTION 1401- NATIONALS AND CITIZENS OF THE UNITED STATES AT BIRTH.

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 C5511.32B.
- 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. The requisite safeguarding requirements are described in Attachment 4 to the basic contract.

2. Definitions

- 2.1. Naval Nuclear Propulsion Information (NNPI) – Per NAVSEAINST C5511.32B: 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 C5511.32B, 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 NNPI hardware as such. This includes seats (desktop and portable), printers and wall plugs.
 - 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 C5511.32B 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).
 - 5.5. 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 C5511.32B).
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.
 - 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 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 NNPI hardware. 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 (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."

- 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 (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.”

- 7.2.3. Splash screens shall require user action to dismiss.
- 7.3. An NMCI user who is not a member of the NNPI COI shall be able to log on to an NMCI seat that is NNPI hardware, shall not be able to access NNPI, and shall be able to access other data and services on NMCI.
- 7.4. A member of the NNPI COI shall be able to log on to an NMCI seat not designated for NNPI, shall not be able to access 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 NNPI COI shall not be permitted to provide read or proxy rights to their e-mail accounts to non-members of the 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 NNPI hardware and is connected to the NMCI in an NNPI workspace.
- 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.

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 require access to only unclassified information and who perform IT duties. Requirements for these investigations are outlined in paragraphs 3-614, 3-710 and Appendix K of DoD 5200.2-R, available at <http://www.ntis.gov>. (Search site: PB2002-107366). Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories below. The contractor shall include all of these requirements in any subcontracts involving IT support.

DoD 5200.28 (Security Requirements for Automated Information Systems (AIS)), paragraph 4.10 which states "Access by foreign nationals to a US government-owned or US Government-managed AIS may be authorized only by the DOD Component Head, and shall be consistent with the DOD, Department of State, and the Director of Central Intelligence policies." The DoD Component Head for the Department of the Navy is the Secretary of the Navy (SECNAV). SECNAV approval is required for all IT access by non-U.S. citizens.

The 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 COR or TR must concur with the designation.

IT-I Position (High Risk) – Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with relatively high risk for causing 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.

IT-II Position (Moderate Risk) - Positions in which the incumbent is responsible for the direction, planning, design, operation or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check (NAC).

IT-III Position (Low Risk) - All other positions involving 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 NAC.

If an employee has a personnel security investigation at the appropriate level without a break in service for more than 24 months, with favorable adjudication, and in the case of IT- I Position is less than 5 years old, you do **not** need to submit an additional investigation for the trustworthiness determination. If required, the contractor will ensure personnel designated IT-I, II, or III complete the Standard Form (SF) 85P. The company shall review the SF 85P for completeness and use Appendix G, SECNAVINST 5510.30A to determine if any adverse information is present. The reviewer shall submit the SF85P to SPAWARSYSCEN San Diego, Code 20351, 53560 Hull Street, San Diego, CA 92152-5001. **Only hard copy SF85Ps are acceptable.** An employee may not begin work on IT until the company receives written notification from Code 20351. For additional assistance please send email to SF85P@spawar.navy.mil.

Specific guidelines for obtaining software of the SF85P are available at <http://www.dss.mil>. If you are unfamiliar with the SF85P, you may send email to SF85P@spawar.navy.mil.

Investigation results shall be returned to SPAWARSYSCEN San Diego, Code 20351, 53560 Hull Street, San Diego, CA 92152-5001 for a trustworthiness determination. SPAWARSYSCEN San Diego will notify the contractor of its decision. The contractor will promptly replace any individual for whom SPAWARSYSCEN San Diego has communicated a negative trustworthiness determination.

The contractor will include the IT Position Category for each person so designated on Visit Authorization Letters (VAL) once the COR or TR has approved the Category and written notification from Code 20351 has been received. VALs will be sent to the following address: Commanding Officer, SPAWARSYSCEN San Diego, ATTN: Code 20352, 49275 Electron Drive, San Diego, CA 92152-5435.

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 with the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program, Operating Manual (NISPOM) available from www.dss.mil. When visiting COMSPAWARSCOM at either Old Town Campus (OTC) or Point Loma Campus (PLC) the Contractor will comply with the security directives used regarding the protection of classified and sensitive but unclassified (SBU) information, SECNAVINST 5510.36 (series) and SECNAVINST 5510.30 (series) both of which are available from <http://neds.nebt.daps.mil/Directives/table52.html>. A hardcopy of these directives will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the SPAWAR Systems Command's Security Contracting Officer's Representative (COR), Code 20351. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location at COMSPAWARSSCOM, the security provisions of the NISPOM will be followed within this cleared facility.

b. Security Supervision. SPAWAR Systems Center will exercise security supervision over all contractors visiting COMSPAWARSSCOM 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 COMSPAWARSSCOM 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 SPAWAR Systems Center 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 at the PLC will immediately report the incident to SPAWAR Systems Center's Code 20351 as well as the Contractor's FSO. An on-site Contractor, whose primary location is OTC, will make their report to Code 20351 as well as the Contractor's FSO. A Code 20351, representative will investigate the circumstances, determine culpability where possible and report results of the inquiry to the FSO and the Cognizant Field Office of the DSS. On-site contractor personnel will promptly correct any deficient security conditions identified by a SPAWAR Systems Center Security representative.

b. Storage.

1. Classified material may be stored in containers authorized by SPAWAR Systems Center's PLC Physical Security Group, Code 20352, or OTC Code 20351, for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board COMSPAWARSSCOM with Code 20352's written permission. Containers to be located at our OTC will request Code 20351's written permission. Areas located within cleared contractor facilities at COMSPAWARSSCOM will be approved by DSS.

2. The use of Open Storage areas must be pre-approved in writing by SPAWAR Systems Center, Code 20352, for the open storage, or processing, of classified material prior to use of that area for open storage. Specific supplemental security controls for open storage areas, when required, will be provided by SPAWAR Systems Center, Code 20352.

c. Transmission of Classified Material.

1. All classified material transmitted by mail for use by long term visitors will be addressed to COMMANDING OFFICER, SPAWAR SYSTEMS CENTER, 53560 HULL ST, 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 COMSPAWARSSCOM by contractor personnel must be delivered to the SPAWAR Systems Center Classified Material Control Center (CMCC), Code 20332, for processing.

3. All CONFIDENTIAL material hand carried to COMSPAWARSSCOM by contractor personnel must be delivered to the Mail Distribution Center, Code 20331, for processing. This applies for either the OTC or PLC sites.

4. All COMSPAWARSSCOM classified material transmitted by contractor personnel from COMSPAWARSSCOM will be sent via the COMSPAWARSSCOM 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 addressed to COMMANDER, ATTN RECEIVING OFFICER CODE 2242, SPAWAR SYSTEMS COMMAND, 4201 PACIFIC HIGHWAY, SAN DIEGO, CA 92110-3127.

III. INFORMATION ASSURANCE (IA) SECURITY. Contractors using Information Systems, networks or computer resources to process classified, SBU or unclassified information will comply with the provisions of SECNAVINST 5239.3 (series) available from <http://neds.nebt.daps.mil/Directives/table48.html> and local policies and procedures. Contractor personnel must ensure that systems they use

at COMSPAWARSYSCOM have been granted a formal letter of approval to operate by contacting their Information System Security Officer (ISSO). A list of ISSOs is available from <https://iweb.spawar.navy.mil/services/security/docs/Issolist.htm>.

IV. VISITOR CONTROL PROCEDURES.

a. Contractor personnel assigned to COMSPAWARSYSCOM will be considered long-term visitors for the purpose of this contract.

b. Submission of valid Visit Authorization Letter (VAL) for classified access to COMSPAWARSYSCOM is the responsibility of the Contractor's Security Office. All VAL's will be prepared in accordance with the NISPOM. They will be sent to either COMMANDING OFFICER, ATTN CODE 20352, SPAWAR SYSTEMS CENTER, 49275 ELECTRON DRIVE, SAN DIEGO, CA 92152-5435 for the PLC, or COMMANDING OFFICER, VISITOR CONTROL OTC, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, SAN DIEGO, CA 92152-5001 for OTC. The VAL's will be addressed to COMSPAWARSYSCOM and list a COMSPAWARSYSCOM point of contact. Visit requests may be sent via facsimile to the PLC at (619) 553-6169, and verified on 553-3203 or the OTC at (619) 524-2745, and verified on 524-2751 or 524-3124.

c. Visit requests for long-term visitors should be received at least one week prior to the expected arrival of the visitor to ensure necessary processing of the request.

d. Code 20352 will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible COMSPAWARSYSCOM COR will request issuance of picture badges to contractor personnel. The COR may, at their discretion, request that picture badges be issued for the length of the basic contract or option period. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Unauthorized use of a COMSPAWARSYSCOM badge will be reported to the DSS. Identification badges must be worn in plain sight at all times on board COMSPAWARSYSCOM.

e. Prior to the termination of a Contractor employee with a COMSPAWARSYSCOM badge or active VAL on file the FSO must:

1. Notify in writing Code 20352 for PLC, Code 20351 for OTC, the COR, 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 emergency situations, 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. Confiscate any COMSPAWARSYSCOM identification badge and vehicle decal and return them to either Code 20352, or Code 20351, no later than 5 working days after the effective date of the termination.

V. INSPECTIONS. Code 20351 personnel will conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel shall cooperate with Code 20351 representatives during these inspections. A report of the inspection will be forwarded to the Contractor's employing facility and COR. The Contractor must be responsive to the Code 20351 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. The Contractor shall ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 20351. This reporting will include the following:

a. The denial, suspension or revocation of security clearance of any assigned personnel;

b. Any adverse information which would cast doubt on an assigned employee's continued suitability for continued access to classified access;

c. Any instance of loss or compromise, or suspected loss or compromise, of classified information;

d. Actual, probable or possible espionage, sabotage, or subversive information; or

e. Any other circumstances of a security nature that would effect the contractor's operation on board COMSPAWARSYSCOM

VII. PHYSICAL SECURITY.

a. SPAWAR Systems Center will provide appropriate response to emergencies occurring onboard this command. The Contractor will comply with all emergency rules and procedures established for COMSPAWARSYSCOM.

b. A roving Contract Security Guard patrol will be accomplished by SPAWAR Systems Center. 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 either PLC Code 20352 or OTC Code 20351.

c. All personnel aboard COMSPAWARSYSCOM AND SPAWAR Systems Center are subject to random inspections of their vehicles, personal items and of them selves. Consent to these inspections is considered to have been given when personnel accept either a badge or a vehicle pass or decal permitting entrance to the command.

VIII. COR RESPONSIBILITIES.

a. Review requests by cleared contractors for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions and/or submit a Final DD 254 to Security's COR.

b. Coordinates, in conjunction with the appropriate transportation element, a suitable method of shipment for classified material when required.

c. Certifies and approves Registration For Scientific and Technical Information Services (DTIC) requests (DD 1540).

d. Ensures that 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, conference registration forms, etc.

IX. SECURITY'S COR RESPONSIBILITIES.

a. Initiate all requests for facility clearance action for our prime contractors with the DSS.

b. Validate justification for Interim Top Secret personnel security clearances and facility clearances.

c. Validate and endorse requests submitted by a cleared contractor for Limited Access Authorizations (LAA) for its non-U.S. citizen employees.

X. SPECIAL CONSIDERATIONS FOR ON-SITE CLEARED FACILITIES.

Any cleared contractor facility on board SPAWARSYSCOM will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional COMSPAWARSYSCOM contracts may be authorized to use this cleared facility, but only on a case-by-case basis. The COR, Security's COR, and Contracting Officer must 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.

XI. ITEMS PROHIBITED ABOARD COMSPAWARSYSCOM/SPAWAR Systems Center.

a. Dangerous weapon, instrument or device includes, but is not limited to, the following:

rifles, automatic rifles, machine guns, sub-machine guns, pistols, machine pistols, flare pistols, starter pistols, shotguns, compressed gas, air or spring fired pellet or "BB" guns, sling shorts, blow guns, or any other device which uses gun powder, compressed gas or air, or spring tension to forcefully eject a projective or other device which may injure someone;

daggers, switch blades, bow and arrows, sear guns, Hawaiian slings, power heads, fishing knives, scuba knives, or any unofficial knife with a blade longer than 2 1/2 inches;

martial arts devices (throwing stars, nunchakus), stun guns, tasers, brass knuckles, billy clubs, night sticks, pipe, bars, or mallets, or other similar devices capable of being used as a weapon;

poison, acids or caustic chemicals;

or any other item that may be used to inflict serious injury or death to another person or temporarily blind or disable an individual injury not specifically authorized by proper authority.

b. Explosive article or compound includes but is not limited to: ammunition for any of the small arms weapons mentioned as a dangerous weapon, including "blank" ammunition, gunpowder, molotov cocktails, pipe bombs, grenades, pyrotechnics, fireworks or any other compound or article which might violently react and cause injury not specifically authorized by proper authority.

c. As an exception to the list of dangerous weapons, the possession of defensive tear gas devices (e.g., pepper spray) aboard all naval installations in California is now permissible. However, unauthorized use of these devices other than for self-defense will be prosecuted as a violation of the Uniform Code of Military Justice or applicable laws.

XII. ESCORTING POLICY.

a. All personnel within COMSPAWARSYSCOM/SPAWAR Systems Center'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 a SPAWAR Systems Center issued badge. The word "Security" or "Safety" on selective Code 2031 or 2038 employee badges authorizes the bearer to escort unbadged emergency vehicles and operators and support personnel during emergencies. Only U.S. citizens and intending citizens (former immigrant aliens) may be escorted under this policy. ALL FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE SPAWAR SYSTEMS COMMAND FOREIGN DISCLOSURE OFFICE, 08-42.

b. All permanently badged COMSPAWARSYSCOM/SPAWAR Systems Center and tenant command employees, as well as those contractors and other government employees who have an "E" for escort on their permanent badges may escort visitors requiring escort.

XIII. CONTRACTOR TRAINING.

All contractor personnel cleared Top Secret, Secret, or Confidential are required to receive annual Security Training. The issuance of a picture badge will trigger an e-mail to be sent to your personnel. This e-mail will give your employee the site of the computer-based training that must be completed. This training is required to be repeated annually.

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 ONI-5, via Security's COR; or
 - c. Release the intelligence material 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 Contracting Officer's Representative (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.

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 SPAWAR Systems Center San Diego CA 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 SPAWAR Systems Center San Diego CA 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 SPAWAR SYSTEMS CENTER SAN DIEGO CA 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 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 to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, is adequate when internal building security is provided during nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.
9. FOUO information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.
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.

TEMPEST REQUIREMENTS QUESTIONNAIRE FOR CONTRACTOR FACILITIES

1. This TEMPEST Requirements Questionnaire (TRQ) must be completed and sent to the contracting authority and the Certified TEMPEST Technical Authority (CTTA) within 30 days after contract award for all contracts where classified National Security Information (NSI) will be processed and the requirements of item 13 of the DD 254 have been met.
2. The prime contractor cannot pass TEMPEST requirements to subcontractors. Subcontractors must submit a Contractor TRQ prior to processing.
3. The TRQ is for information collection only. It is not a directive or an implied requirement, nor is it an encouragement to procure TEMPEST equipment or any type of shielding for use on this contract. Do not initiate any changes to equipment of facilities for TEMPEST unless it has been recommended by the CTTA and specifically directed by the contracting authority.
4. The contracting authority will not issue any directives concerning TEMPEST until after the contractor submitted TRQ has been evaluated by the CTTA and resulting recommendations received. To fully evaluate the TRQ, the CTTA may request additional information concerning the facility, its physical control, the equipment which will be used to process NSI, etc.
5. The contractor shall ensure compliance with any TEMPEST countermeasure(s) specifically directed in writing by the contracting authority.
6. Please provide the information requested in paragraphs 7 through 20 and return to the CTTA at:

Commanding Officer
SPAWARSYSCEN Charleston
Code 723
PO Box 190022
North Charleston, SC 29419-9022
7. Provide the name, address, position title and phone number (at the facility where classified processing will occur) of a point of contact who is knowledgeable of the processing requirements, the types of equipment to be used and the physical layout of the facility.
8. Provide the specific geographical location, address, and zip code, where classified processing will be performed.
9. What are the classification level(s) of material to be processed/handled by electronic or electromechanical information system(s) and what percentage is processed at each level?
10. What special categories of classified information are processed?
11. Is there a direct connection (wire line or fiber) to a Radio Frequency (RF) transmitter(s) located either locally or at a remote site?
12. Are there any RF transmitters located within 6 meters of the system processing National Security Information or the system's RED signal lines?
13. Describe how access is controlled to your facility including the building, compound, plant, property, and/or parking lots. Where are visitor's first challenged/identified? Include controls such as alarms, guards, patrols, fences and warning signs. Provide a simple block diagram of the equipment, the facility and the surrounding areas. The

diagram(s) should extend out to the nearest uncontrolled area on each side of the facility, such as a military base perimeter, plant property line, commercial building or residential area.

14. Are there other tenants in the building who are not U.S. department/agencies or their agents?
15. Are there any known foreign business or government offices in adjacent buildings?
16. Provide the make and model number of all equipment used to process, transfer or store classified information. Include computers, peripherals, network servers, network hardware, multiplexers, modems, encryption devices (COMSEC), etc.
17. Have on-site TEMPEST tests been conducted on any of these equipment(s)? If so, which ones? When was the test(s) conducted? Who conducted the test(s)? Have all deficiencies (if any) been resolved?
18. Has a TEMPEST Facility Zoning test been conducted? If so, who conducted the testing and when?
19. Is this company foreign-owned or controlled? If so, what is the country?
20. Provide the name, code, telephone number, and address of the Contracting Officer's Representative, the contract number and the sponsoring command.

NOV 07 '01 23:28PM 123

P.2



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

IN REPLY REFER TO

4200

Ser 114-01

30 OCT 2001

MEMORANDUM

From: Director, Intelligence-Related Contracting Coordination
Office (IRCCO)
To: Commander, Space and Naval Warfare Systems Center (SPAWAR),
San Diego (Roger Aronoff)
Subj: INTELLIGENCE-RELATED CONTRACTING (IRC) REQUEST SPAWAR ltr Ser
D0173/020-01 dated 11 Jul 01
Ref: (a) SECNAVINST C4200.35 of 1 Mar 01
Encl: (1) IRC REQUEST NAVSEA ltr Ser D0172/020-01 dated 11 Jul 01

1. The request for Intelligence-Related Contracting (IRC) support contained in enclosure (1) has been reviewed in detail. It is our understanding that the basic contract with EDS has already been awarded by SPAWAR and being administered by SPAWAR. However, when Intelligence Related taskings arise and need to be supported by cleared individuals for contract administration prior coordination with the IRCCO is required.
2. The IRC Coordinating Office (IRCCO) point of contact for this transaction is Denise Schafer who may be contacted at telephone (301) 669-2060. Our IRCCO reference number is 114-01

A handwritten signature in black ink, appearing to read "T. W. Essig".

T. W. ESSIG
Acting

FOR OFFICIAL USE ONLY

SECNAVINST C4290.35
01 Mar 2001

4. AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY

a. Does this contract require development, delivery, support or use of AIS systems and/or networks that will process SCI/other sensitive information? **NO**

b. Has the proper authority accredited AIS and/or networks? **N/A**

If Yes, by whom?
If No, contact SSO Navy for guidance

5. ADMINISTRATIVE SECURITY

a. Does the contractor require access to SCI documents or other sensitive material to support this contract? **YES**

If Yes, list specific SCI documents requiring release to the contractor. Identify specific subject areas of SCI/other sensitive material required.

Information system threat assessments, including source, means, and suspected mechanisms that attacks will be promulgated. Information is required to assess NMCI vulnerabilities and develop counter-strategies to mitigate vulnerabilities and threats.

b. Does the contractor require SCI/other manuals, directives, indoctrination tapes, oaths, cover sheets, technical classification guides, etc.? **NO**

If Yes, list specific items.

SSO Navy will provide these items to the contractor.

Samuel A. Richardson / 6 Nov 01
SSO NAVY VALIDATION/DATE

EDS / N00094-00-D-6000
Contract/Subcontract No.

[Signature] 06/21/01
Contract Monitor Signature and Date

CLASSIFICATION: Unclassified

6/14

Sub-Contractor Special Security Officer
Name:
Phone:

e. Brief description of required service or product:

The NMCI will provide secure, comprehensive, end to end information services through a common computing and communications environment that supports the Department of the Navy's core business, scientific, executive management, and information activities. It will enhance interoperability and information exchange capability for Navy and Marine Corps users, as well as our level and deployed forces.

f. Justify the need-to-know for each SCI program (e.g., SI/TK, etc.), or sensitive mission revealing information required in support of this contract.

- 1) *In order to protect and defend NMCI from known or suspected attacks, vulnerabilities must be eliminated. Access to TS/SCI information is critical in addressing these vulnerabilities.*
- 2) *NMCI personnel will require access to NIPRNET/SIPRNET systems that reside within a SCIF. Unescorted access within SCIFs is essential in order to sustain required levels of support.*

3. **PHYSICAL SECURITY**

a. SCIF REQUIREMENTS:

(1) List all locations where contract work will be performed.
Various Government SCI Facilities throughout CONUS. NMCI will be implemented at all DON commands within CONUS and the Contractor will be required to access SCIFs at all DON commands that maintain them.

- | | |
|--|-----|
| (2) Is an accredited contractor SCIF required? | NO |
| If yes, has a fixed facility checklist or concept approval been sent to DIA? | N/A |
| If answer to (2) is NO, proceed to Section 4. CUI Security | |
| (3) Is an accredited contractor SCIF presently available for use on this contract? | NO |
| If No, has a pre-construction checklist been submitted to DIA? | N/A |
| (4) Is a Co Utilization Agreement (CUA) required? | NO |
| (5) With what other agency (if known) ? | |
| (6) Has a CUA already been executed? | N/A |

If No, attach a request for a CUA for processing by SSO Navy.

b. What categories of SCI/other sensitive material will be used/stored at the contractor's SCIF? *N/A*

SI _____ TK _____ OTHER _____ NONE _____
(be specific)

c. If a co-utilization of an existing SCIF is required, what is the estimated volume of SCI/other sensitive material to be stored at the contractor's SCIF? *N/A*

CLASSIFICATION: Unclassified



SECNAVINST C4200.35

01 Mar 2001

IRC REQUIREMENTS CHECKLISTCLASSIFICATION Unclassified (ACCORDING TO CONTENT)**1. IRC REQUIREMENTS CHECKLIST**

- a. Does the Statement of Work (SOW) and/or contract contain requirements for SCI? **YES**
- b. Does the SOW accurately describe the efforts to be performed? **YES**
(Note: If SCI is to be utilized in contract performance, it must be identified in the SOW)
- c. Is the contract product SCI? **NO**
- d. Does the contract performance require use/storage of SCI at the Contractor's SCIF? **NO**
- e. Does the contract performance require:
- (1) Substantial access to SCI areas or materials at U.S. Govt SCIFs? **YES**
(Note: Substantial Access refers to a contract that requires knowledge of sensitive intelligence collection sources and methods or analytical or operational intelligence capabilities)
- (2) Other than substantial access to SCI areas, information or systems? **N/A**
- (3) Only entry and unescorted access within U.S. Govt SCIFs? **YES (some)**
- f. Do the Government Contracting Activity (GCA) administrative personnel, in performance of contract award administration and other oversight functions, require access to SCI? **NO**
- g. Does the contracting effort, although non-SCI and non-compartmented, reveal sensitive operations or missions? **NO**

2. CONTRACT INFORMATIONa. Contractor Name: *EDS*Address: *13600 EDS Drive, Herndon, VA 20171*Contract Number: *N00024-00-D-6000*Unclassified Title: *Navy / Marine Corps Intranet (NMCI)*

b. Contracting Officer Representative (COR) certifying IRC requirements:

Name: *Kevin P. McNally*Activity: *SPAWARSSYSCOM*Code: *PMW 164-4*Phone: *(COMM) (619) 524-7580 (DSN) 524-7580*

c. Contractor Project Manager:

Name: *Rick Rosenburg*Phone: *(703) 736-8546*

Contractor Special Security Officer

Name: *Walt Nagurny*Phone: *(703) 736-3425*

d. Sub-Contractor Name:

Address:

Sub-Contract Number:

Unclassified Title:

Sub-Contractor Project Manager

Name:

Phone:

CLASSIFICATION: Unclassified