

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED <p style="text-align: center;">TOP SECRET</p> b. LEVEL OF SAFEGUARDING REQUIRED <p style="text-align: center;">SECRET</p>			
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	<input checked="" type="checkbox"/>	a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD)	20100709		
	b. SUBCONTRACT NUMBER		b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO.	DATE (YYYYMMDD)		
<input checked="" type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER N00039-10-R-0001	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		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
THIS DD254 IS FOR SOLICITATION PURPOSES ONLY. A TAILORED ORIGINAL DD254 WILL BE PROVIDED UPON CONTRACT AWARD.							
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
8. ACTUAL PERFORMANCE							
a. LOCATION		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>				
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT THIS IS A CONTRACT FOR THE PROVISION OF COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS, INTELLIGENCE SURVEILLANCE, AND RECONNAISSANCE (C4ISR) INSTALLATION SERVICES WORLDWIDE AT DOD FACILITIES AND ON A WIDE VARIETY OF MOBILE PLATFORMS SUCH AS SURFACE SHIPS AND SUBMARINES.							
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY			<input checked="" type="checkbox"/>
b. RESTRICTED DATA			<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY			<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<input checked="" type="checkbox"/>	
d. FORMERLY RESTRICTED DATA			<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>	
e. INTELLIGENCE INFORMATION			<input checked="" type="checkbox"/>	e. PERFORM SERVICES ONLY		<input checked="" type="checkbox"/>	
(1) Sensitive Compartmented Information (SCI)		<input checked="" type="checkbox"/>		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<input checked="" type="checkbox"/>	
(2) Non-SCI		<input checked="" type="checkbox"/>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER			<input checked="" type="checkbox"/>
f. SPECIAL ACCESS INFORMATION			<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>	
g. NATO INFORMATION		<input checked="" type="checkbox"/>		i. HAVE TEMPEST REQUIREMENTS		<input checked="" type="checkbox"/>	
h. FOREIGN GOVERNMENT INFORMATION			<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/>	
i. LIMITED DISSEMINATION INFORMATION			<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>	
j. FOR OFFICIAL USE ONLY INFORMATION		<input checked="" type="checkbox"/>		l. OTHER <i>(Specify)</i>		<input checked="" type="checkbox"/>	
k. OTHER <i>(Specify)</i> SEE PAGE 3.		<input checked="" type="checkbox"/>		SEE BLOCK 13 FOR ELECTRONIC MEDIA REQUIREMENTS.			

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 (COMSPAWARSSYSCOM), CODE 8.5, 4301 PACIFIC HIGHWAY, SAN DIEGO CA 92110-3127

RELEASE OF COMSEC AND SCI INFORMATION 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.*)

SOLICITATION/CONTRACT NUMBER: N00039-10-R-0001.

CLASSIFICATION GUIDES: OPNAVINST S5513.6D COMMUNICATIONS AND SATELLITE PROGRAMS (NAVY PROGRAMS APPLY) ACCESS REQUIREMENTS TO BE PROVIDED UNDER SEPARATE COVER BY COMSPAWARSSYSCOM 4.0.

ACCESS REQUIREMENTS: (CONTINUED ON PAGES 3 AND 4)

THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) FOR SSC ATLANTIC FOR COLLATERAL/SCI IS MR. ROBERT BEEBE, CODE 42B00, 843-218-4911

THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) FOR SSC PACIFIC IS MR. WILLIAM STEWART, CODE 42110, 619-524-2485 AND THE ACOR IS MS. JOCELYN NIMUAN, CODE 42110, 619 524-3120/619 524-2782.

THE SCI COR FOR SSC PACIFIC IS KEVIN CASE, CODE 42110, 619 524-3386.

THE PROCUREMENT CONTRACTING OFFICER (PCO) RICK ESAIAS, CODE 2.1.1, 619 524-7183, THE CONTRACTING SPECIALIST IS MATTHEW FLEMING, CODE 2.1.A4, 619 524-7091.

COPIES OF ALL SUBCONTRACT DD FORM 254S MUST BE PROVIDED TO THE SSC ATLANTIC COR CODE 42B00; SSC PACIFIC CODES COR CODE 42110; ACOR CODE 42110; SCI COR CODE 42110; PCO CODE 2.1.1, AND CODE 83310 SECURITY (RENIE.YTURRALDE@NAVY.MIL).

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 which 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. (CONTINUED ON PAGE 4)

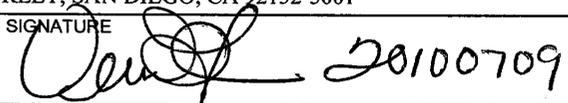
15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No
 (*If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.*)

CSO AND INSPECTION AUTHORITY FOR SCI IS DIRECTOR, OFFICE OF NAVAL INTELLIGENCE (523), 4251 SUITLAND ROAD, WASHINGTON, DC 20395-5720 TELEPHONE (301) 669-2060. DSS IS RELIEVED OF SECURITY INSPECTION RESPONSIBILITY FOR ALL SUCH MATERIAL BUT RETAINS RESPONSIBILITY FOR ALL NON-SCI CLASSIFIED MATERIAL RELEASED TO OR DEVELOPED UNDER THIS CONTRACT AND HELD WITHIN A CONTRACTOR'S SCIF.

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 VERNA F. MINARD	b. TITLE SECURITY'S COR	c. TELEPHONE (<i>Include Area Code</i>) 619 553-3005
---	----------------------------	---

d. ADDRESS (*Include Zip Code*)
 COMMANDING OFFICER, SPACE AND NAVAL WARFARE SYSTEMS CENTER (SSC PACIFIC), CODE 83310, 53560 HULL STREET, SAN DIEGO, CA 92152-5001

e. SIGNATURE


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 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

SOLICITATION/CONTRACT NUMBER: N00039-10-R-0001 /**BLOCK 13 CONTINUED:****PAGE 3 OF 4**

OTHER LOCATIONS OF PERFORMANCE OF WORK WILL BE MULTIPLE DOD, A DEPARTMENT OF HOMELAND SECURITY SITES AND ON MOBILE PLATFORMS THROUGHOUT THE WORLD AS IDENTIFIED ON TASK ORDERS TO BE AWARDED.

10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF THE SPACE AND NAVAL WARFARE SYSTEMS CENTER PACIFIC (SSC PACIFIC) TECHNICAL CODE AND SPACE AND NAVAL SYSTEMS CENTER ATLANTIC (SSC ATLANTIC) 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. (ACCESS IS FOR COMSEC EQUIPMENT AND SIPRNET.)**

10.E(1) DSS IS RELIEVED OF SECURITY INSPECTION RESPONSIBILITY FOR ALL SUCH MATERIAL BUT RETAINS RESPONSIBILITY FOR ALL NON-SCI CLASSIFIED MATERIAL RELEASED TO OR DEVELOPED UNDER THIS CONTRACT. ALL SCI WORK WILL BE PERFORMED AT A GOVERNMENT SCIF. PRIOR APPROVAL OF THE SSC PACIFIC AND/OR SSC ATLANTIC TECHNICAL CODE IS REQUIRED FOR SUBCONTRACTING.

10.E(2) PRIOR APPROVAL OF THE SSC PACIFIC AND/OR SSC ATLANTIC TECHNICAL CODE IS REQUIRED FOR SUBCONTRACTING.

10.G CONTRACTOR IS REQUIRED TO BE BRIEFED AND GRANTED ACCESS TO NATO FOR THE SOLE PURPOSE OF ACCESSING SIPRNET. THIS ACCESS MUST BE NOTED IN JPAS IAW CNO LTR 5510 SER N09N2/8U223003. ACCESS TO NATO INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL AND A SPECIAL BRIEFING. THE SPECIAL BRIEFING IS PROVIDED BY THE CONTRACTING COMPANY'S FACILITY SECURITY OFFICER. NOTE: THERE IS NO REQUIREMENT FOR THE CONTRACTOR TO HAVE ACCESS TO NATO MATERIAL ON THIS CONTRACT.

10.K NEED ACCESS TO NUCLEAR WORK AREAS AND CONTROLLED NUCLEAR INFORMATION AREAS TO PERFORM WORK. NO ACCESS IS REQUIRED FOR NUCLEAR WEAPON DESIGN INFORMATION.

11.C ALL CLASSIFIED MATERIAL MUST BE MARKED IN ACCORDANCE WITH EXECUTIVE ORDER E.O. 13526 DTD 5 JANUARY 2010 AND CNO LTR N09N2/8U223000 DTD 7 JAN 08. NOTE: EXEMPTION CATEGORIES X1 THROUGH X8 DECLASSIFICATION MARKINGS ARE NO LONGER USED.

11.D APPROXIMATELY 8 CUFT OF GSA APPROVED STORAGE WILL BE REQUIRED ON THIS CONTRACT.

11.E CONTRACT IS FOR INSTALLATION ENGINEERING, IMPLEMENTATION, AND SUPPORT SERVICES. CLEARED PERSONNEL MAY BE REQUIRED TO PERFORM THESE SERVICES FOR SOME TASK ORDERS BECAUSE ESCORTING PERSONNEL OR SANITIZATION OF THE WORK SPACES CANNOT PRECLUDE ACCESS TO CLASSIFIED INFORMATION. PERSONNEL CLEARANCE REQUIREMENTS WILL BE PROVIDED BY TASK ORDER, FOR ANY TASK WITH SECURITY CLEARANCE REQUIREMENTS BEYOND THOSE STATED IN THE CONTRACT STATEMENT OF WORK AND CONTRACT PERSONNEL QUALIFICATIONS. ANY CLASSIFICATION GUIDANCE NEEDED WILL BE PROVIDED BY COMSPAWARSYSCOM, SSC PACIFIC OR SSC ATLANTIC DEPENDING UPON WHERE WORK IS PERFORMED.

11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS LOCATIONS: NAPLES & GAETA, ITALY; MANAMA, BAHRAIN; YOKOSUKA & SASEBO, JAPAN; ROTA, SPAIN; SOUDA BAY, GREECE; SINGAPORE; DIEGO GARCIA, BRITISH INDIAN OCEAN TERRITORY ; KOREA; AND POSSIBLY OTHER OVERSEAS LOCATIONS. 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. 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://WWWA.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.H THE CONTRACTOR IS REQUIRED TO HAVE A COMSEC ACCOUNT AT CONTRACTOR'S FACILITY.

11.K THE CONTRACTOR SHALL MAKE ARRANGEMENTS TO USE THE SERVICES OF THE DCS FOR TRANSPORTATION OF QUALIFIED MATERIAL. THE CONTRACTING ACTIVITY WILL REQUEST DCS SERVICES FROM COMMANDER, DCS, ATTN: OPERATIONS DIVISION, FORT GEORGE MEADE, MD 20755-5370. TO OBTAIN DCS GUIDANCE REFER TO THE DOD DIRECTIVE 5200.33, DEFENSE COURIER SERVICE LOCATED AT <http://www.dtic.mil/whs/directives/corres/pdf/520033r.pdf>.

SOLICITATION/CONTRACT NUMBER: N00039-10-R-0001 /**BLOCK 13 CONTINUED:****PAGE 4 OF 4**

11.L THE USE OF PERSONAL ELECTRONIC MEDIA (COMPUTER LAPTOPS, FLASH (THUMB), OR OTHER REMOVABLE DRIVES) IS PROHIBITED IN ALL DEPARTMENT OF DEFENSE ORGANIZATION SPACES EXCEPT WHERE EXPLICITLY PERMITTED BY THEIR ORGANIZATION'S INFORMATION ASSURANCE MANAGER (COMSPAWARSYSCOM, DIRECTOR OF SECURITY, (858) 537-8898, SSC PACIFIC SSCSD_ACCREDIT@NAVY.MIL AND DESIGNATED PERSONNEL AT SSC ATLANTIC) WHERE WORK IS BEING PERFORMED. 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.

THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) OR TECHNICAL REPRESENTATIVE (TR) WILL SPECIFY WHICH POSITIONS REQUIRE CLEARANCE.

BLOCK 14 CONTINUED:

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS ARE ATTACHED AND **MUST** BE PASSED TO SUBCONTRACTORS.

TEMPEST REQUIREMENTS QUESTIONNAIRE IS ATTACHED AND MAY BE PASSED TO SUBCONTRACTORS.

INTELLIGENCE REQUIREMENTS ARE ATTACHED.

FOUO REQUIREMENTS ARE ATTACHED.

OPSEC REQUIREMENTS ARE ATTACHED.

NO FURTHER ENTRIES ON THIS PAGE.



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 125-10
4 Jun 10

MEMORANDUM

From: Coordinator, Intelligence-Related Contracting Coordination Office (IRCCO), Arlington
To: Special Security Office, SPAWAR San Diego, ATTN: R. Aronoff

Subj: GLOBAL C4ISR

Ref: (a) SECNAVINST C4200.35 of 1 Mar 01

Encl: (1) SSO Navy Validation

1. In accordance with the requirements of reference (a) the subject matter has been reviewed in detail and does not meet the IRC criteria for the following reasons:

- a. Contract deliverables will not be SCI;
 - b. Contract statement of work is not SCI.
2. The point of contact is Daphne Moore at (703) 699-4440.

Kevin Reilly
KEVIN REILLY

FOR OFFICIAL USE ONLY

CLASSIFICATION: _____
(Unclassified until filled-in)

SECNAVINST C4200.35
1 Mar 2001
SD Revision - Oct 2005

Ken B. Ladd 22 Apr 10

Contract Monitor Signature and Date
Solicitation # N00039-10-R-0001

Margaret Nelson 7/1/10

SSO Navy Validation and Date

Contract #:

SubContract #:

Prime Contractor:

SubContractor:

125-10

CLASSIFICATION: _____

12-11
FOR OFFICIAL USE ONLY

Form (c)

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/dir.html>. 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 Program Executive Office, Command, Control, Communications, Computer and Intelligence (PEO C4I) 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 PEO C4I 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 (NAC).

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 NAC.

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 NACI 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 FD 258 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 SF85P@spawar.navy.mil.

Visit Authorization Letters (VALs) for Qualified Employees:

Contractors that have been awarded a classified 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 VALS. Therefore, contractors who work on classified 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 Space and Naval Warfare Systems Center Pacific use its 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 (DSS guidance dated 24 April 2007, subject: ***Procedures Governing The Use Of JPAS By Cleared Contractors***).

Employment Terminations:

The contractor shall:

- Immediately notify the COR or TR of the employee's termination.
- Fax a termination VAL to Code 83320 at (619) 553-6169.
- Return any badge and decal to Code 83320.

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, Command, Control, Communications, Computers and Intelligence (PEO C4I) 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 NRADINST 5720.1(series). Both of the SECNAV Instructions are available online at <http://neds.nebt.daps.mil/directives/table52.html>. A copy of NRADINST 5720.1 will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the PEO C4I Security's Contracting Officer's Representative (COR), Code 83351. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location from PEO C4I, the security provisions of the NISPOM will be followed within this cleared facility.
- b. **Security Supervision.** SSC Pacific will exercise security supervision over all contractors visiting PEO C4I 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 C4I 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 SSC 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 SSC 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 SSC Pacific Security representative.
- b. **Storage.**
 1. Classified material may be stored in containers authorized by SSC 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 C4I with Code 83320's written permission. Areas located within cleared contractor facilities on board PEO C4I 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 SSC 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: 271582-SN00, SSC 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 C4I 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 C4I by contractor personnel that is intended to remain at PEO C4I shall be provided to the designated recipient or proper cleared PEO C4I employee.
 4. All PEO C4I classified material transmitted by contractor personnel from PEO C4I will be sent via the PEO C4I 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, 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 C4I have been granted a formal letter of approval to operate by contacting their Information Assurance Office.

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.

IV. VISITOR CONTROL PROCEDURES.

- a. Contractor personnel assigned to PEO C4I will be considered long-term visitors for the purpose of this contract.
- b. Contractors that have been awarded a classified 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 VALs. Therefore, contractors who work on classified 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 SPAWAR Systems Center Pacific use its 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/> (DSS guidance dated 24 April 2007, subject: **Procedures Governing the Use of JPAS by Cleared Contractors**).

- c. For visitors to receive a SPAWAR Systems Center Pacific 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 C4I 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 SSC Pacific badge will be reported to the DSS.
- f. Prior to the termination of a Contractor employee with a SSC 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 SSC 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.

The Contractor will ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 83310. If further investigation is warranted it will be conducted by Code 83310. 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 effect the contractor's operation on board COMSPAWARSYSCOM.

- 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. SSC Pacific will provide appropriate response to emergencies occurring onboard this Command. The Contractor will comply with all emergency rules and procedures established for SSC Pacific.
- b. A roving Contract Security Guard patrol will be provided by SSC 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 SSC 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.
- c. Information about parking restrictions may be found on the Security web site at <https://dsp.spawar.navy.mil/domino/iweb/instructions.nsf/InstructionsByRef/5560-1>.

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. COR 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 C4I will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional PEO C4I 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 C4I AND SSC PACIFIC.

The following items are prohibited within any PEO C4I & SSC Pacific 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 SSC Pacific 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 C4I and SSC 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 C4I , 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 C4I and SSC 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 SSC Pacific issued badge. Only U.S. citizens and U.S. Permanent Residents may be escorted under this policy. ALL COMSPAWARSYSCOM FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE COMSPAWARSYSCOM FOREIGN VISITS COORDINATOR OFFICE, 8335. Contact phone number: (858) 537-8884.
- b. All pictured badged PEO C4I 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.
- d. 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.

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 Command 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 Command 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 COMMAND 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, 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.

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.

TEMPEST REQUIREMENTS QUESTIONNAIRE (TRQ) FOR CONTRACTOR FACILITIES

1. This 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 Atlantic
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 (wireline 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 NSI 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

**TEMPEST REQUIREMENTS QUESTIONNAIRE (TRQ)
FOR CONTRACTOR FACILITIES**

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/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 hardware, multiplexors, 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 contract number, identify the sponsoring command, point of contact or Contracting Officer's Representative, and their telephone number.

OPERATIONS SECURITY REQUIREMENTS

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

- | | |
|--|---|
| <ul style="list-style-type: none"> - National Security Decision Directive 298 - DOD 5205.02 - OPNAVINST 3432.1 - SPAWARINST 3432.1 | <ul style="list-style-type: none"> -National Operations Security Program (NSDD) 298 -DOD Operations Security (OPSEC) Program -DON Operations Security -Operations Security Policy |
|--|---|

The contractor will accomplish the following minimum requirements in support of Space and Naval Warfare Systems Command (SPAWAR) Operations Security (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 SPAWAR 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 SPAWAR, 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 also information as identified by SPAWAR or the SPAWAR Security COR.
- SPAWAR 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 (Pk), 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. (greater than 3 days in advance).
 - Details of SPAWAR/SSC Pacific/SSC Atlantic 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.
 - Force Protection specific capabilities or response protocols (timelines/equipment/numbers of personnel/training received/etc.).
 - Command leadership and VIP agendas, reservations, plans/routes etc.
 - Detailed facility maps or installation overhead photography (photo with annotation of Command areas or greater resolution than commercially available).
 - Details of COOP, SPAWAR/SSC Pacific/SSC Atlantic emergency evacuation procedures, or emergency recall procedures.
 - Government personnel information that would reveal force structure and readiness (such as recall rosters or deployment lists).
 - 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 contractor's 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 SPAWAR Security COR (who will consult with the SPAWAR/SSC Pacific/SSC Atlantic OPSEC Manager).
- All above requirements MUST be passed to all Sub-contractors.