

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING			
<i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				a. FACILITY CLEARANCE REQUIRED SECRET			
				b. LEVEL OF SAFEGUARDING REQUIRED SECRET			
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>			3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>				
a. PRIME CONTRACT NUMBER		X		a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD) 20101229		
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)		
X	c. SOLICITATION OR OTHER NUMBER N00039-11-R-0059	DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>	DATE (YYYYMMDD)		
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.							
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____							
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>							
a. NAME, ADDRESS, AND ZIP CODE THIS DD 254 IS FOR SOLICITATION PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE PROVIDED UPON CONTRACT AWARD.		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip)</i>			
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip)</i>			
8. ACTUAL PERFORMANCE							
a. LOCATION		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip)</i>			
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT LEASED SATELLITE UHF NARROWBAND BANDWIDTH AND TRACKING, TELEMETRY, AND COMMAND (TT&C) SERVICES.							
10. CONTRACTOR WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY			X
b. RESTRICTED DATA			X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL			X
d. FORMERLY RESTRICTED DATA			X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE			X
e. INTELLIGENCE INFORMATION:				e. PERFORM SERVICES ONLY			X
(1) Sensitive Compartmented Information (SCI)			X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES			X
(2) Non-SCI			X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER			X
f. SPECIAL ACCESS INFORMATION			X	h. REQUIRE A COMSEC ACCOUNT			X
g. NATO INFORMATION			X	i. HAVE TEMPEST REQUIREMENTS			X
h. FOREIGN GOVERNMENT INFORMATION			X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X	
i. LIMITED DISSEMINATION INFORMATION			X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE			X
j. FOR OFFICIAL USE ONLY INFORMATION		X		l. OTHER <i>(Specify)</i> ELECTRONIC MEDIA REQUIREMENTS		X	
k. OTHER <i>(Specify)</i>			X				

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, CODE 8.5.1, 4301 PACIFIC HIGHWAY, SAN DIEGO CA 92110-3127

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.

* In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

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

CLASSIFICATION GUIDES:

OPNAVINST 5513.6D, 06-21, SATELLITE COMMUNICATIONS, FLEET (FLTSATCOM)

ACCESS REQUIREMENTS:

THE CONTRACTING OFFICER IS MARK LOPEZ, SPAWAR 2.1.3, TELEPHONE 619-524-7168

THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) IS MAJ RODGER PITT, PEO SS 6.0, TELEPHONE 858-537-8619

THE CONTRACTING SPECIALIST IS KAT STARON-BARABASZ, SPAWAR 2.0, TELEPHONE 858-537-0433

11.L THE USE OF PERSONAL ELECTRONIC MEDIA (COMPUTER LAPTOPS, FLASH (THUMB), OR OTHER REMOVABLE DRIVES) IS PROHIBITED IN TEAM SPAWAR SPACES EXCEPT WHERE EXPLICITLY PERMITTED BY THE COMSPAWARSYSCOM DIRECTOR OF SECURITY, (858) 537-8898. ALL REMOVABLE ELECTRONIC MEDIA MUST BE LABELED (UNCLASSIFIED, ETC.) TO THE HIGHEST CLASSIFICATION OF DATA STORED, AND/OR FOR THE CLASSIFICATION OF THE SYSTEM IN WHICH IT IS USED. IF CLASSIFIED, ANY REMOVABLE ELECTRONIC MEDIA MUST BE TRACKED AND STORED APPROPRIATE TO THAT LEVEL OF CLASSIFICATION.

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

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

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

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

FOR OFFICIAL USE ONLY (FOUO) GUIDANCE ATTACHED.

OPERATIONS SECURITY (OPSEC) REQUIREMENTS ATTACHED.

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

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

a. TYPED NAME OF CERTIFYING OFFICIAL

P. A. TALLEY
PATTI.TALLEY@NAVY.MIL

b. TITLE

SECURITY'S CONTRACTING OFFICER'S
REPRESENTATIVE (COR)

c. TELEPHONE (*Include Area Code*)

(619) 221-4529

d. ADDRESS (*Include Zip Code*)

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

e. SIGNATURE

20101229



17. REQUIRED DISTRIBUTION

- a. CONTRACTOR
- b. SUBCONTRACTOR
- c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR

- d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- e. ADMINISTRATIVE CONTRACTING OFFICER CODE 2.0 (LOPEZ)
- f. OTHERS AS NECESSARY SPAWAR CODES 8.3.3, PEO SS 6.0 (PITT)

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

Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated every 5 years by using the Electronic Questionnaire for Investigation Processing (eQIP) web based program (SF86 format).

IT-II Position (Limited Privileged)

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

- Access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts;
- Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year. Other positions are designated by Space and Naval Warfare Systems Command that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT-I positions. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudicated National Agency Check (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 an FD258 Fingerprint Card or electronic fingerprint transmission

The company's Facility Security Officer (FSO) is responsible for completing the following items located on the top portion of the SF85P: 1) Clearly indicate for item "A" if the Trustworthiness Investigation is for an 08B (IT-II position) or an 02B (IT-III position); 2) item "B" Extra Coverage enter R, this will allow the Government to request for the finger print data quickly so that a Common Access Card (CAC) can be processed if needed. 3) item "C" is for the Sensitivity/Risk Level enter either 1 (low risk positions), 5 (moderate risk positions), or 6 (high risk positions); 4) item "D" for Computer/ADP (IT) enter I, II, or III; 5) item "E" for the Nature of Action Code enter CON; 6) item "I" must contain the name of the position and the contract number; 7) item "J" SON enter 4219; 8) item "K" place and X by "None"; 9) item "L" SOI enter NV00; 10) item "M" place and X by "None"; 11) item "N" type DOD-NAVY; 12) item "O" Accounting-Data and/or Agency Case Number enter contracting facility's Cage Code; and 13) item "P" Company representatives/FSO are **NOT** to sign the SF85P, you must leave this blank.

The company shall review the SF85P for completeness and use SECNAV M-5510.30, Appendix G available at <https://doni.daps.dla.mil/secnavmanuals.aspx> to determine if any adverse information is present. Additional guidance for requesting investigations from OPM is found at <http://www.opm.gov>. Completed SF85P packages will be mailed "in care of" to: Commanding Officer, Space and Naval Warfare Systems Center Pacific, Code 83310 (SF85P), 53560 Hull Street, San Diego, CA 92152-5001.

Note: All forms must be signed by the individual within 60 days of the date of submission. Submitted forms, which are not received within these 60 days, will be delayed or returned. If no change has occurred, forms must be re-dated and initialed by the Subject/employee. If the SF85P is submitted with missing information or adverse information is found, the form(s) will be returned to the company/FSO to revised and resubmit.

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

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

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

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 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 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 OR THE AUTHOR. When the FOUO status is terminated you will be notified.

7. You may disseminate FOUO information to your employees and subcontractors who have a need for the Information in connection with this contract.

8 During working hours, reasonable steps should be taken to minimize risk of access by unauthorized personnel. FOUO Information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, or similar items.

9. FOUO information may be transmitted via first-class mail, parcel post, fourth-class mail for bulk shipments only.

10. When no longer needed, FOUO information may be disposed by tearing each copy into pieces to preclude reconstructing and placing it in a regular trash, or recycle, container or in the uncontrolled burn.

11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO Information protected by the Privacy Act may result in criminal sanctions.

12. Electronic transmission of FOUO Information (voice, data, or facsimile) should be by approved secure communications systems whenever practical.

13. To obtain for official use only (FOUO) guidance refer to the DoD Information Security Program Regulation, DoD 5200.1-r, appendix 3, located at <http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf>.

OPERATIONS SECURITY (OPSEC) REQUIREMENTS

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

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

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

- The contractor will practice OPSEC and implement OPSEC countermeasures to protect DoD Critical Information. Items of Critical Information are those facts, which individually, or in the aggregate, reveal sensitive details about SPAWARSYSCOM or the contractor's security or operations related to the support or performance of this SOW, and thus require a level of protection from adversarial collection or exploitation not normally afforded to unclassified information.
- Contractor must protect Critical Information and other sensitive unclassified information and activities, especially those activities or information which could compromise classified information or operations, or degrade the planning and execution of military operations performed or supported by the contractor in support of the mission. Protection of Critical Information will include the adherence to and execution of countermeasures which the contractor is notified by or provided by SPAWARSYSCOM, for Critical Information on or related to the SOW.
- Sensitive unclassified information is that information marked FOR OFFICIAL USE ONLY (or FOUO), Privacy Act of 1974, Company Proprietary, and information identified by SPAWARSYSCOM or the SPAWARSYSCOM Security Representative.
- SPAWARSYSCOM has identified the following items as Critical Information that may be related to this SOW:
 - Known or probable vulnerabilities to any U.S. system and their direct support systems.
 - Details of capabilities or limitations of any U.S. system that reveal or could reveal known or probable vulnerabilities of any U.S. system and their direct support systems.
 - Details of information about military operations, missions, and exercises.
 - Details of U.S. systems supporting combat operations (numbers of systems deployed, deployment timelines, locations, effectiveness, unique capabilities, etc.).
 - Operational characteristics for new or modified weapon systems (Probability of Kill, Countermeasures, Survivability, etc.).
 - Required performance characteristics of U.S. systems using leading edge or greater technology (new, modified, or existing).
 - Telemetered or data-linked data or information from which operational characteristics can be inferred or derived.
 - Test or evaluation information pertaining to schedules of events during which Critical Information might be captured. (advance greater than 3 days).
 - Details of Team SPAWAR unique Test or Evaluation capabilities (disclosure of unique capabilities).
 - Existence and/or details of intrusions into or attacks against DoD Networks or Information Systems, including, but not limited to, tactics, techniques and procedures used, network vulnerabilities exploited, and data targeted for exploitation.
 - Network User ID's and Passwords.
 - Counter-IED capabilities and characteristics, including success or failure rates, damage assessments, advancements to existing or new capabilities.
 - Vulnerabilities in Command processes, disclosure of which could allow someone to circumvent security, financial, personnel safety, or operations procedures.
 - 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, Team SPAWAR 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 contractors ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the NISPOM. NSDD 298, DoD 5205.02, "DOD Operations Security (OPSEC) Program", and OPNAVINST 3432.1, "Operations Security" should be used to assist in creation or management of training curriculum.

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

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

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