DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED
SECRET

b. LEVEL OF SAFEGUARDING REQUIRED
NONE

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER N00039-16-R-0006	DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)* 20151027
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE *(YYYYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ 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? ☐ YES ☒ 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 *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip)*
THIS DD 254 IS FOR SOLICITATION PURPOSES ONLY. AN ORIGINAL DD 254 WILL BE PROVIDED UPON CONTRACT AWARD.		

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

DEVELOP THE CAPACITY AS A SERVICE (CAAS) MODEL OR "UTILITY" MODEL FOR COMPUTE, STORAGE, AND NETWORKING.

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 (Specify) CONTROLLED UNCLASSIFIED INFORMATION (CUI) HANDLING REQUIREMENTS	X	
k. OTHER (Specify)		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 (SPAWARSYSCOM), 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.)*

ACCESS REQUIREMENTS:

THE CONTRACTING OFFICER IS ED MCGINNIS, SPAWAR 2.1, (619) 524-7197
THE CONTRACTING OFFICER'S REPRESENTATIVE (COR) IS DAVID EDWARDS, SSC LANT, (843) 218-7033

11.A CONTRACT PERFORMANCE IS RESTRICTED TO SSC LANT AND SSC PAC SPACES. COMMANDER, SPAWAR SYSTEMS COMMAND WILL PROVIDE SECURITY CLASSIFICATION GUIDANCE FOR PERFORMANCE OF THIS CONTRACT.

11.L CONTRACTORS RECEIVING, TRANSMITTING OR ACCESSING CONTROLLED UNCLASSIFIED INFORMATION (CUI) ON OR THROUGH ITS CONTRACTOR INFORMATION SYSTEM(S) MUST SAFEGUARD THE INFORMATION TO AVOID COMPROMISE, INCLUDING BUT NOT LIMITED TO DISCLOSURE OF INFORMATION TO UNAUTHORIZED PERSONS, UNAUTHORIZED MODIFICATION, DESTRUCTION, OR LOSS OF AN OBJECT, OR THE COPYING OF INFORMATION TO UNAUTHORIZED MEDIA, AS REQUIRED PER DFARS SUBPART 204.73 AND CLAUSES 204.7304 AND 252.204-7012. CONTRACTORS SHALL REPORT TO THE DOD EACH CYBER INCIDENT THAT AFFECTS UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION RESIDENT ON OR TRANSITING CONTRACTOR INFORMATION SYSTEMS IN ACCORDANCE WITH DFARS CLAUSE 204.7304 AND 252.204-7012. DETAILED REPORTING CRITERIA AND REQUIREMENTS ARE SET FORTH IN THE CLAUSE AT 252.204-7012, SAFEGUARDING OF UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION.

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

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

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

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

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	b. TITLE	c. TELEPHONE *(Include Area Code)*
ALICIA RHAMY ALICIA.RHAMY@NAVY.MIL	SECURITY'S CONTRACTING OFFICER'S REPRESENTATIVE (COR)	(619) 221-7638

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

e. SIGNATURE
Alicia Rhamy
20151027

17. REQUIRED DISTRIBUTION
☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER SPAWAR CODE 2.1 (MCGINNIS)
☒ f. OTHERS AS NECESSARY CODES 8.3.3, SSC LANT (EDWARDS)

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 with Local Agency Check and Credit Check (NACLC) which is submitted using the eQIP web based program (SF86 format) .

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 NACLC which is submitted using the eQIP web based program (SF86 format) or a NACI (SF85 format).

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 investigation to support IT access will normally not be required. If an individual is cleared, but does not have a completed SSBI and is determined to be an IT-I, then a SSBI will be submitted using the eQIP web based program (SF86 format). 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 appropriate investigation.

Employment Terminations:

The contractor shall:

- Immediately notify the COR or TR of the employee's termination.

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 Space and Naval Warfare Systems Command (SPAWARSYSCOM) 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). Both of the SECNAV Instructions are available online at http://neds.nebt.daps.mil/directives/table52.html. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location from SPAWAR SYSCOM, the security provisions of the NISPOM will be followed within this cleared facility.

b. Security Supervision. SPAWARSYSCOM will exercise security supervision over all contractors visiting SPAWARSYSCOM 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 SPAWARSYSCOM 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 SPAWAR HQ Code 83310, telephone (619) 221-7638, as well as the Contractor's FSO. A Code 833 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 SPAWARSYSCOM Security representative.

b. Storage.

1. Classified material may be stored in containers authorized by SPAWARSYSCOMSOM Access Control Office for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board SPAWARSYSCOM with Code 833's written permission. Areas located within cleared contractor facilities on board SPAWARSYSCOM 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 SPAWARSYSCOM.

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: SSC Pacific: 271582-SN00, SSC Pacific.

(b) CONFIDENTIAL and SECRET material transmitted by FedEx, USPS Registered, Express mail will be addressed to COMMANDER, SPACE & NAVAL WARFARE SYSTEMS COMMAND,

4301 PACIFIC HWY, SAN DIEGO CA 92110-3127. 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 SPAWARSYSCOM 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 SPAWARSYSCOM by contractor personnel that is intended to remain at SPAWARSYSCOM shall be provided to the designated recipient or proper cleared SPAWARSYSCOM employee.

4. All SPAWARSYSCOM classified material transmitted by contractor personnel from SPAWARSYSCOM will be sent via the SPAWARSYSCOM 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 SYSTEMS (IS) Security. Contractors using ISs, 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 SPAWARSYSCOM have been granted a formal letter of approval to operate by contacting their Information Assurance Office.

IV. VISITOR CONTROL PROCEDURES.

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

a. 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 SSC 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)***.

b. 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.

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. The Contractor must be responsive to the Code 83310 representative's findings.

VI. REPORTS. As required by the NISPOM, Chapter 1, Section 3, contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), the status of an employee's personnel clearance (PCL), the proper safeguarding of classified information, or an indication classified information has been lost or compromised.

a. The Contractor will ensure that certain information pertaining to assigned contractor personnel or operations is reported to Security's COR, Code 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 affect the contractor's operation on board SPAWARSYSCOM.

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

VII. PHYSICAL SECURITY.

a. 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 SPAWARSYSCOM 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.

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 SPAWARSYSCOM will be used strictly for official business associated with this contract. No other work may be performed aboard this facility. Additional SPAWARSYSCOM 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 SPAWARSYSCOM AND SSC Pacific.

The following items are prohibited within any SPAWARSYSCOM & 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 SPAWARSYSCOM 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 SPAWARSYSCOM, 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 Commander is granted.

Personnel desiring to hold a social function and serve alcohol, should send a memo (hard copy) to the Commander, 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 SPAWARSYSCOM foreign national visitors must be processed through the SPAWAR foreign visits coordinator office, 8335. Contact phone number: (858) 537-8884.

XIII. CELLULAR PHONE USAGE.

a. Cellular phone use is prohibited in all secure spaces, i.e. Open Storage areas, classified laboratories.

b. Vehicle operators on DoD installations and operators of Government vehicles shall not use cellular phones, unless the vehicle is safely parked or unless they are using a hands-free device, and are also prohibited from wearing of any other portable headphones, earphones, or other listening devices while operating a motor vehicle.

c. The use of cellular phones, portable headphones, earphones, or other listening devices while jogging, walking bicycling, or skating on roads and streets on Navy installations is prohibited except for use on designated bicycle and running paths and sidewalks.

XIV. PERSONAL ELECTRONIC MEDIA

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

FOR OFFCIAL 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 9of the Freedom of Information Act (FOIA).

2. Use of FOUO markings doesn't mean that the information can't be released to the public, only that it must be reviewed by PEO C4I prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

3. An UNCLASSIFIED document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the bottom face and interior pages.

4. Classified documents containing FOUO do not require any markings on the face of the document; however, the interior pages containing only FOUO information shall be marked top and bottom center with "FOR OFFICIAL USE ONLY" Mark only unclassified portions containing FOUO with "(FOUO)" immediately before the portion.

5. Any FOUO information released to you by PEO C4I is required to be marked with the following statement prior to transfer:

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

6. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. DO NOT REMOVE ANY FOUO MARKING WITHOUT WRITTEN AUTHORIZATION FROM PEO C4I 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.
- <u>SPAWARSYSCOM has identified the following items as Critical Information that may be related to this SOW</u>:
    - 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 SPAWARSYSCOM Security Representative (who will consult with the SPAWARSYSCOM 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 .