

| DEPARTMENT OF DEFENSE<br>CONTRACT SECURITY CLASSIFICATION SPECIFICATION   |  |                   |  | 1. CLEARANCE AND SAFEGUARDING  |               |
|---|--|-------------------|--|--|---------------|
| (The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)  |  |                   |  | a. FACILITY CLEARANCE REQUIRED<br>SECRET   |               |
|   |  |                   |  | b. LEVEL OF SAFEGUARDING REQUIRED<br>NONE  |               |
| 2. THIS SPECIFICATION IS FOR: (X and complete as applicable)  |  |                   | 3. THIS SPECIFICATION IS: (X and complete as applicable) |  |               |
|   | a. PRIME CONTRACT NUMBER                         | X                 | a. ORIGINAL (Complete date in all cases)                 | Date (YYMMDD)<br>20011108  |               |
|   | b. SUBCONTRACT NUMBER                            |                   | b. REVISED (Supersedes all previous specs)               | Revision No.   | Date (YYMMDD) |
| X   | c. SOLICITATION OR OTHER NO.<br>N66001-02-R-5021 | Due Date (YYMMDD) | c. FINAL (Complete Item 5 in all cases)                  | Date (YYMMDD)  |               |
| 4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following:<br>Classified material received or generated under (Preceding Contract Number) is transferred to this follow-on contract.   |  |                   |  |  |               |
| 5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following:<br>In response to the contractor's request dated , retention of the identified classified material is authorized for the period of   |  |                   |  |  |               |
| 6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)  |  |                   |  |  |               |
| a. NAME, ADDRESS, AND ZIP CODE<br>THIS DD 254 IS FOR SOLICITATION PURPOSES ONLY.<br>AN ORIGINAL DD 254 WILL BE PROVIDED UPON CONTRACT AWARD.  |  | b. CAGE CODE      | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)        |  |               |
| 7. SUBCONTRACTOR  |  |                   |  |  |               |
| a. NAME, ADDRESS, AND ZIP CODE  |  | b. CAGE CODE      | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)        |  |               |
| 8. ACTUAL PERFORMANCE   |  |                   |  |  |               |
| a. NAME, ADDRESS, AND ZIP CODE  |  | b. CAGE CODE      | c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)        |  |               |
| 9. GENERAL IDENTIFICATION OF THIS PROCUREMENT   |  |                   |  |  |               |
| IDENTIFICATION OF RESEARCH AND EXPLORATORY DEVELOPMENTAL EFFORTS INVOLVING EMERGING NAVIGATION TECHNOLOGIES WITH POTENTIAL FOR APPLICABILITY IN THE AREAS OF SENSORS AND SYSTEMS, AND AIR AND SHIPBOARD COMMAND, CONTROL, COMMUNICATION, COMPUTERS AND INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (C4ISR) SYSTEM TECHNOLOGIES. |  |                   |  |  |               |
| 10. THIS CONTRACT WILL REQUIRE ACCESS TO:   |  | YES               | NO   | 11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:  |               |
| a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION   |  | X                 |  | a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY                    | X             |
| b. RESTRICTED DATA  |  |                   | X  | b. RECEIVE CLASSIFIED DOCUMENTS ONLY   |               |
| 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   |               |
| (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  |               |
| g. NATO INFORMATION   |  |                   | X  | i. HAVE TEMPEST REQUIREMENTS   |               |
| h. FOREIGN GOVERNMENT INFORMATION   |  | X                 |  | j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS   |               |
| 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)   |               |
| k. OTHER (Specify)  |  |                   |  |  |               |
| SAP NO.: 100000440  |  |                   |  |  |               |

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

DIRECT  THROUGH (Specify):

COMMANDING OFFICER, SPAWAR SYSTEMS CENTER D003, 53560 HULL STREET, SAN DIEGO CA 92152-5001

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:**

10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF SPAWAR SYSTEMS CENTER SAN DIEGO CA. 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.

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

10.H PRIOR APPROVAL OF SPAWAR SYSTEMS CENTER SAN DIEGO CA IS REQUIRED FOR SUBCONTRACTING. ACCESS TO CLASSIFIED FOREIGN GOVERNMENT INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL. ACCESS IS LIMITED TO INFORMATION FROM THE UNITED KINGDOM.

11.A CONTRACT PERFORMANCE IS RESTRICTED TO SPAWAR SYSTEMS CENTER SAN DIEGO CA AND SPAWAR SYSTEMS CENTER SAN DIEGO CA WILL PROVIDE SECURITY CLASSIFICATION GUIDANCE FOR PERFORMANCE OF THIS CONTRACT.

11.E CONTRACT IS FOR ENGINEERING SERVICES. CLEARED PERSONNEL ARE REQUIRED TO PERFORM THIS SERVICE BECAUSE ACCESS TO CLASSIFIED INFORMATION CAN NOT BE PRECLUDED BY ESCORTING PERSONNEL.

11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS LOCATIONS: THE UNITED KINGDOM. ANTI-TERRORISM/FORCE PROTECTION BRIEFINGS ARE REQUIRED FOR ALL PERSONNEL PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL. THE BRIEFING IS AVAILABLE ON OUR WEBSITE AT [HTTPS://IWEB.SPAWAR.NAVY.MIL/SERVICES/SECURITY/TRAINING/INDEX.HTML](https://iweb.spawar.navy.mil/services/security/training/index.html).

11.G THE CONTRACTOR IS AUTHORIZED THE USE OF DTIC AND WILL PREPARE AND PROCESS DD FORM 1540 IN ACCORDANCE WITH THE NISPOM, CHAPTER 11, SECTION 2. THE COR WILL CERTIFY NEED-TO-KNOW TO DTIC. ONLY UNCLASSIFIED INFORMATION MAY BE OBTAINED THROUGH DTIC.

ALL REQUESTS FOR INFORMATION SHOULD BE DIRECTED TO THE CONTRACTING OFFICER D211, TELEPHONE (619) 553-4462.

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

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

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed)

SPECIFIC ON-SITE SECURITY REQUIREMENTS ARE ATTACHED.

INTELLIGENCE REQUIREMENTS ARE ATTACHED.

FOR OFFICIAL USE ONLY (FOUO) INFORMATION IS ATTACHED.

INFORMATION TECHNOLOGY (IT) PERSONNEL SECURITY PROGRAM REQUIREMENTS IS 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  
 PATTI@SPAWAR.NAVY.MIL  
 P. A. TALLEY

b. TITLE  
 SECURITY'S CONTRACTING OFFICER'S  
 REPRESENTATIVE (COR)

c. TELEPHONE (Include Area Code)  
 (619) 553-3195

d. ADDRESS (Include Zip Code)  
 COMMANDING OFFICER  
 SPAWAR SYSTEMS CENTER D0351  
 53560 HULL ST.  
 SAN DIEGO, CA 92152-5001

e. SIGNATURE

20011115



**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 D211
- f. OTHERS AS NECESSARY D0351, D313

## INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS

The U.S. Government conducts trustworthiness investigations of personnel who require access to only unclassified information and who perform IT duties. Requirements for these investigations are outlined in paragraphs 3-614, 3-710 and Appendix K of DoD 5200.2-R, available at <http://www.ntis.gov/product/dod-directives.htm>. Personnel occupying an IT Position shall be designated as filling one of the IT Position Categories below. The contractor shall include all of these requirements in any subcontracts involving IT support.

According to DoDD 5200.28 (Security Requirements for Automated Information Systems), paragraph 4.10 which states "Access by foreign nationals to a US government-owned or US Government-managed AIS may be authorized only by the DOD Component Head, and shall be consistent with the DOD, Department of State, and the Director of Central Intelligence policies." SECNAV approval is required for all non-U.S. citizens. All requests requiring SECNAV approval shall be submitted to D0351.

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

**IT-I Position (High Risk)** – Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realizing significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR). The SSBI or SSBI-PR shall be updated every 5 years.

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

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

If an employee has a personnel security investigation at the appropriate level without a break in service for more than 24 months, with favorable adjudication, and in the case of IT- I Position is less than 5 years old, you do **not** need to submit an additional investigation for the trustworthiness determination. If required, the contractor will ensure personnel designated IT-I, II, or III complete the Standard Form (SF) 85P. The company shall review the SF 85P for completeness and use Appendix G, SECNAVINST 5510.30A to determine if any adverse information is present. If adverse information is present the company may submit a "Request for Waiver", along with the SF 85P, to allow their employee to work on this contract. The "Request for Waiver" must contain the name of the employee, their SSN, justification, contract number, name and telephone number of the COR, and IT Position Category assigned. The reviewer shall submit the SF85P, and a "Request for Waiver" if applicable, to SPAWARSCEN San Diego, Code D0351, 53560 Hull Street, San Diego, CA 92152-5001. **Only hard copy SF85Ps are acceptable.** An employee may not begin work on IT until the company receives written notification from D0351. For additional assistance please send email to SF85P@spawar.navy.mil.

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

Investigation results shall be returned to SPAWARSCEN San Diego, Code D0351, 53560 Hull Street, San Diego, CA 92152-5001 for a trustworthiness determination. SPAWARSCEN San Diego will notify the contractor of its decision. The contractor will promptly replace any individual for whom SPAWARSCEN San Diego has communicated a negative trustworthiness determination.

The contractor will include the IT Position Category for each person so designated on Visit Authorization Letters (VAL) once the COR or TR has approved the Category and written notification from D0351 has been received. VALs will be sent to the

## 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 SPAWAR Systems Center at either the Point Loma Campus (PLC) or Old Town Campus (OTC) the Contractor will comply with the security directives used regarding the protection of classified and sensitive unclassified information, SECNAVINST 5510.36 (series), SECNAVINST 5510.30 (series), and NOSCINST 5720.2 (series). A copy of these directives will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the SPAWAR Systems Center's Security Contracting Officer's Representative (COR), Code D0351. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location at SPAWAR Systems Center, the security provisions of the NISPOM will be followed within this cleared facility.

b. Security Supervision. SPAWAR Systems Center will exercise security supervision over all contractors visiting SPAWAR Systems Center 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 SPAWAR Systems Center are responsible for the control and safeguarding of all classified material in their possession. All contractor personnel will be briefed by their FSO on their individual responsibilities to safeguard classified material. In addition, all contractor personnel are invited to attend SPAWAR Systems Center conducted Security Briefings, available at this time by appointment only. In the event of possible or actual loss or compromise of classified material, the on-site Contractor will immediately report the incident to SPAWAR Systems Center's Code D0351 as well as the Contractor's FSO. A Code D0351 representative will investigate the circumstances, determine culpability where possible and report results of the inquiry to the FSO and the Cognizant Field Office of the DSS. On-site contractor personnel will promptly correct any deficient security conditions identified by a SPAWAR Systems Center Security representative.

#### b. Storage.

1. Classified material may be stored in containers authorized by SPAWAR Systems Center's PLC Physical Security Group, Code D0352 for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board SPAWAR Systems Center PLC with Code D0352's written permission. Areas located within cleared contractor facilities on board SPAWAR Systems Center will be approved by DSS.

2. The use of Open Storage areas must be pre-approved in writing by Code D0352 for the open storage, or processing, of classified material prior to use of that area for open storage. Specific supplemental security controls for open storage areas, when required, will be provided by SPAWAR Systems Center, Code D0352.

#### c. Transmission of Classified Material.

1. All classified material transmitted by mail for use by long term visitors will be addressed to COMMANDING OFFICER, SPAWAR SYSTEMS CENTER, 53560 HULL ST, SAN DIEGO CA 92152-5001. The inner envelope will be addressed to the attention of the Contracting Officer's Representative (COR) or applicable Technical Representative (TR) for this contract, to include their code number.

2. All SECRET material hand carried to SPAWAR Systems Center by contractor personnel must be delivered to the Classified Material Control Center (CMCC), Code D0332, for processing.

3. All CONFIDENTIAL material hand carried to SPAWAR Systems Center by contractor personnel must be delivered to the Mail Distribution Center, Code D0331, for processing. This applies for either the OTC or PLC sites.

4. All SPAWAR Systems Center classified material transmitted by contractor personnel from the SPAWAR Systems Center will be sent via the SPAWAR Systems Center COR or TR for this contract.

5. The sole exception to the above is items categorized as a Data Deliverable. All contract Data Deliverables will be addressed to COMMANDING OFFICER, ATTN RECEIVING OFFICER CODE D20C, SPAWAR SYSTEMS CENTER, 53560 HULL ST, SAN DIEGO, CA 92152-5410.

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 SPAWAR Systems Center have been granted a formal letter of approval to operate by contacting their Information System Security Officer (ISSO).

#### IV. VISITOR CONTROL PROCEDURES.

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

b. Submission of valid Visit Authorization Letter (VAL) for classified access to SPAWAR Systems Center is the responsibility of the Contractor's Security Office. All VAL's will be prepared in accordance with the NISPOM. They will be sent to either COMMANDING OFFICER, ATTN CODE D0352, SPAWAR SYSTEMS CENTER, 49275 ELECTRON DRIVE, SAN DIEGO, CA 92152-5435 for the PLC, or COMMANDING OFFICER, VISITOR CONTROL OTC, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, SAN DIEGO, CA 92152-5001 for OTC. Visit requests may be sent via facsimile to the PLC at (619) 553-6169, and verified on 553-3203 or the OTC at (619) 524-2745, and verified on 524-2751 or 524-3124. Visit requests may be submitted for the length of the basic contract or option period.

c. 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.

d. Code D0352 will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible SPAWAR Systems Center COR will request issuance of picture badges to contractor personnel. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Unauthorized use of an SPAWAR Systems Center badge will be reported to the DSS. Identification badges must be worn in plain sight at all times on board SPAWAR Systems Center.

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

1. Notify in writing Code D0352, the COR, Security's COR, and the laboratory managers of any laboratories into which the employee had been granted unescorted access of the termination and effective date. In emergency situations, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.

2. Confiscate any SPAWAR Systems Center identification badge and vehicle decal and return them to Code D0352 no later than 5 working days after the effective date of the termination.

V. INSPECTIONS. Code D0351 personnel will conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel will cooperate with Code D0351 representatives during these inspections. A report of the inspection will be forwarded to the Contractor's employing facility and COR. The Contractor must be responsive to the Code D0351 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 D0351. This reporting will include the following:

- a. The denial, suspension or revocation of security clearance of any assigned personnel;
- b. Any adverse information that would cast doubt on an assigned employee's continued suitability for continued access to classified access;
- c. Any instance of loss or compromise, or suspected loss or compromise, of classified information;
- d. Actual, probable or possible espionage, sabotage, or subversive information; or
- e. Any other circumstances of a security nature that would effect the contractor's operation on board SPAWAR Systems Center.

#### VII. PHYSICAL SECURITY.

- a. SPAWAR Systems Center will provide appropriate response to emergencies occurring onboard this Division. The Contractor will comply with all emergency rules and procedures established for SPAWAR Systems Center.
- b. A roving Contract Security Guard patrol will be accomplished by SPAWAR Systems Center. Such coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Specific questions or concerns should be addressed to Code D0352.
- c. All personnel aboard SPAWAR Systems Center are subject to random inspections of their vehicles, personal items and of them selves. Consent to these inspections is given when personnel accept either a badge or a vehicle pass/decal permitting entrance to this command.

#### VIII. COR RESPONSIBILITIES.

- a. Review requests by cleared contractors for retention of classified information beyond a 2-year period and advise the contractor of disposition instructions and/or submit a Final DD 254 to Security's COR.
- b. Coordinates, in conjunction with the appropriate transportation element, a suitable method of shipment for classified material when required.
- c. Certifies and approves Registration For Scientific and Technical Information Services requests (DD 1540) (DTIC).
- d. Ensures that timely notice of contract award is given to host commands when contractor performance is required at other locations.
- e. Certify need-to-know on visit requests and conference registration forms.

#### IX. SPECIAL CONSIDERATIONS FOR ON-SITE CLEARED FACILITIES.

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

- a. Dangerous weapon, instrument or device includes, but is not limited to, the following:  
rifles, automatic rifles, machine guns, sub-machine guns, pistols, machine pistols, flare pistols, starter pistols, shotguns, compressed gas, air or spring fired pellet or "BB" guns, sling shorts, blow guns, or any other device which uses gun powder, compressed gas or air, or spring tension to forcefully eject a projective or other device which may injure someone;

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

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

poison, acids or caustic chemicals;

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

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

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

#### XI. ESCORTING POLICY.

a. All personnel within SPAWAR Systems Center's fenced perimeters, with the exception of emergency personnel such as fire, ambulance, or hazardous material response personnel responding to an actual emergency, must wear an SPAWAR Systems Center issued badge. The word "Security" or "Safety" on selective Code D035 or D038 employee badges authorizes the bearer to escort unbadged emergency vehicles and operators and support personnel during emergencies. Only U.S. citizens and Permanent Residents (former immigrant aliens) may be escorted under this policy. ALL FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE SPAWAR SYSTEMS CENTER FOREIGN DISCLOSURE OFFICE, D0351.

b. All permanently badged SPAWAR Systems Center and tenant command employees, as well as those contractors and other government employees who have an "E" on their red and blue, respectively back grounded permanent badges may escort those visitors requiring an escort-required badge.

#### XIII. CONTRACTOR TRAINING.

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

## FOR OFFICIAL USE ONLY (FOUO) INFORMATION

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

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA.  
EXEMPTION(S) \_\_\_\_\_ APPLY.
6. Removal of the FOUO marking can only be accomplished by the originator or other competent authority. DO NOT REMOVE ANY FOUO MARKING WITHOUT WRITTEN AUTHORIZATION FROM SPAWAR SYSTEMS CENTER SAN DIEGO CA OR THE AUTHOR. When the FOUO status is terminated you will be notified.
7. You may disseminate FOUO information to your employees and subcontractors who have a need for the information in connection with this contract.
8. During working hours FOUO information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During nonworking hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks, is adequate when internal building security is provided during nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.
9. FOUO information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.
10. When no longer needed, FOUO information may be disposed by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash, or recycle, container or in the uncontrolled burn.
11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

## CONTRACTOR REQUIREMENTS FOR ACCESS TO INTELLIGENCE INFORMATION

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