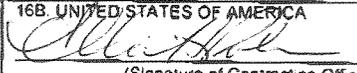


AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE N00024-00-D-6000	PAGE OF 1	PAGES 1
2. AMENDMENT/MODIFICATION NO P00005	3. EFFECTIVE DATE See Block 16C	4. REQUISITION/PURCHASE REQUISITION NO. N/A		5. PROJECT NO N/A	
6. ISSUED BY SPACE AND NAVAL WARFARE SYSTEMS COMMAND (SPAWAR) Contracting Officer: ELLEN H. POLEN 4301 PACIFIC HIGHWAY, OT-4, ROOM 2082B SAN DIEGO, CA 92110-3127 PHONE: (619)524-7388		7. ADMINISTERED BY (if other than Item 6) SAME AS BLOCK 6			
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) ELECTRONIC DATA SYSTEMS 13600 EDS DRIVE HERNDON, VA 20171 Attn: NMCI Contracts		(x)	9A. AMENDMENT OF SOLICITATION NO.		
		X	9B. DATED (SEE ITEM 11)		
			10A. MODIFICATION OF CONTRACT/ORDER N00024-00-D-8000		
			10B. DATED (SEE ITEM 13) 08 OCT 00		
CODE IU305	FACILITY CODE				
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input checked="" type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of offers <input checked="" type="checkbox"/> is <input type="checkbox"/> is not extended. Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation as amended, by the following checked method: (a) By completing Items 8 and 15, and returning ___ copies of the amendment; <input checked="" type="checkbox"/> (b) By acknowledging receipt of this amendment on each copy of the offer submitted, or (c) By separated letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (if required) N/A					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIED THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.					
(x)	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify Authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT/ORDER NO. IN ITEM 10A.				
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).				
<input checked="" type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: By Mutual Agreement of the parties				
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)				
E. IMPORTANT: Contractor <input type="checkbox"/> is not <input checked="" type="checkbox"/> is required to sign this document and return 2 copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)					
The purpose of this modification is to revise Attachment 7, DD Form 254 in its entirety. This revised DD254 provides access to NATO SECRET information. The revised Attachment 7, DD Form 254, Rev. 1, is attached hereto.					
A CONFORMED COPY OF THE REVISED CONTRACT INCLUSIVE OF THE REVISED ATTACHMENT 7, DD FORM 254, IS MADE A PART OF THIS MODIFICATION AS A RESULT OF THE CHANGES OUTLINED HEREIN.					
All other terms and conditions of Contract N00024-00-D-6000 remain unchanged, and in full force and effect.					
Except as provide herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.					
15A. NAME AND TITLE OF SIGNER (Type or Print) Keith Spencer, NMCI Contracts Manager			16A. NAME AND TITLE OF SIGNER (Type or Print) Ellen H. Polen, Contracting Officer		
15B. CONTRACTOR/OFFEROR  (Signature of person authorized to sign)		15C. DATE SIGNED 22 MAR 2001	16B. UNITED STATES OF AMERICA  (Signature of Contracting Officer)		16C. DATE SIGNED 22 Mar 01

NSN 7540-010152-9070  
PREVIOUS EDITION UNUSABLE

STANDARD FORM 30 (REV. 10-83)  
Prescribed by GSA

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)				a. FACILITY CLEARANCE REQUIRED TOP SECRET	
				b. LEVEL OF SAFEGUARDING REQUIRED SECRET	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)		
X	a. PRIME CONTRACT NUMBER N00024-00-D-6000	X	a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 000830	
	b. SUBCONTRACT NUMBER	X	b. REVISED (Supersedes all previous specs)	Revision No. 1	Date (YYMMDD) 010125
	c. SOLICITATION OR OTHER NO.		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:					
Classified material received or generated under _____ (Preceding Contract Number) is transferred to this follow on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If Yes, complete the following:					
In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE ELECTRONIC DATA SYSTEMS CORPORATION 13600 EDS DRIVE A5N-E31 HERNDON, VA 20171-3225		b. CAGE CODE 1U305	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip) DEFENSE SECURITY SERVICE (DSS) NORTHEAST REGION 7010 LITTLE RIVER TURNPIKE, SUITE 310 ANNANDALE, VA 22003-0308		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)		
8. ACTUAL PERFORMANCE					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, Zip)		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT					
NAVY MARINE CORPS INTRANET					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
b. RESTRICTED DATA			X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA			X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
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	
(2) Non-SCI		X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
f. SPECIAL ACCESS INFORMATION			X	h. REQUIRE A COMSEC ACCOUNT	
g. NATO INFORMATION SECRET		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	
j. FOR OFFICIAL USE ONLY INFORMATION		X		l. OTHER (Specify) AIS CLASSIFIED PROCESSING	
k. OTHER (Specify)			X		
PR NO.:					

PR NO.:

CONTRACT NUMBER: N00024-00-D-6000

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

DIRECT  THROUGH (Specify): **RELEASE OF COMSEC INFORMATION IS NOT AUTHORIZED.**

COMMANDER, SPAWAR SYSTEMS COMMAND, 00L, 4301 PACIFIC HIGHWAY, SAN DIEGO CA 92110-3127

Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.

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

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

**CLASSIFICATION GUIDES: (GUIDE(S) PROVIDED UNDER SEPARATE COVER BY TECHNICAL REPRESENTATIVE, PMW 164-4)**  
 OPNAVINST S5513.10B, ENCL 12, NAVAL COMPUTER SECURITY (FORMERLY SECURITY, ADP)  
 NMCI SECURITY REQUIREMENTS, MAY 2000 (attached)

- ACCESS REQUIREMENTS:**
- 10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF COMSPAWARSYSCOM. ACCESS TO ANY COMSEC INFORMATION REQUIRES SPECIAL BRIEFINGS AT THE CONTRACTOR FACILITY. ACCESS TO CLASSIFIED COMSEC INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL.
  - 10.E(2) PRIOR APPROVAL OF COMSPAWARSYSCOM IS REQUIRED FOR SUBCONTRACTING. ACCESS TO INTELLIGENCE INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL.
  - 10.G ACCESS TO NATO INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL AND SPECIAL BRIEFINGS. HIGHEST LEVEL IS NATO SECRET.
  - 11.C MAJORITY OF CLASSIFIED WORK/STORAGE DONE AT A GOVT FACILITY AND/OR OTHER APPROVED/CLEARED CONTRACTOR. FACILITY INFORMATION GENERATED IN PERFORMANCE OF THIS DELIVERY ORDER SHALL BE MARKED IN ACCORDANCE WITH E.O. 12958.
  - 11.D RESTRICTED/CLOSED AREAS AND/OR GSA APPROVED SECURITY CONTAINER(S) WILL BE REQUIRED.
  - 11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS LOCATIONS: GUANTANAMO BAY (CUBA), PUERTO RICO, AND ICELAND.
- ANTI-TERRORISM/FORCE PROTECTION BRIEFINGS REQUIRED FOR PERSONNEL PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL.**

-----BLOCK 13 ACCESS CONTINUED ON NEXT PAGE-----

TECHNICAL REPRESENTATIVE: KEVIN P. McNALLY, PMW 164-4, (619) 524-7580

**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  YES  NO 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 ATTACHED.  
 INTELLIGENCE INFORMATION REQUIREMENTS ATTACHED.  
 AUTOMATED INFORMATION SYSTEM (AIS) PERSONNEL SECURITY PROGRAM REQUIREMENTS FOR OFFICIAL USE ONLY (FOUO) INFORMATION ATTACHED.  
 CONTRACTOR TEMPEST QUESTIONNAIRE ATTACHED AND MAY BE PASSED TO SUBCONTRACTORS.

**15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office.  YES  NO (If Yes, explain and identify specific areas or elements carved out and the actively 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 CASWELL@SPAWAR.NAVY.MIL CHRISTINE CASWELL	b. TITLE SECURITY CONTRACTING OFFICER'S REPRESENTATIVE (COR)	c. TELEPHONE (Include Area Code) (619) 524-2672
--	---	--

d. ADDRESS (Include Zip Code) COMMANDING OFFICER SPAWAR SYSTEMS CENTER CODE D0355 53560 HULL ST. SAN DIEGO, CA 92152-5001	<b>17. REQUIRED DISTRIBUTION</b> <input checked="" type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
---	--

e. SIGNATURE 010125 	<input checked="" type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input checked="" type="checkbox"/> f. OTHERS AS NECESSARY D0355, PMW 164-4
--	---

BLOCK 13 ACCESS REQUIREMENTS CONTINUED:

11.G THE CONTRACTOR IS AUTHORIZED THE USE OF DTIC REGARDING CONTRACT RELATED MATTER AND WILL PREPARE AND PROCESS DD FORM 1540 IN ACCORDANCE WITH THE NISPOM, CHAPTER 11, SECTION 2. THE COR WILL CERTIFY NEED-TO-KNOW TO DTIC.

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

11L. CLASSIFIED AIS PROCESSING SHALL BE IN ACCORDANCE WITH THE PROVISIONS OF THE NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM), CHAPTER 8, AND MUST BE PERFORMED ON AN ACCREDITED COMPUTER SYSTEMS APPROVED BY DSS.

VISIT REQUESTS TO OTHER THAN COMSPAWARSYSCOM SHALL HAVE "NEED TO KNOW" CERTIFIED BY TECHNICAL REPRESENTATIVE, PMW 164-4.

**ELECTRONIC DATA SYSTEMS CORPORATION**  
**SPECIFIC ON-SITE SECURITY REQUIREMENTS**  
N00024-00-D-6000

I. GENERAL.

a. Contractor Performance. In performance of this Contract the following security services and procedures are incorporated as an attachment to the DD Form 254. The Contractor will conform with the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program, Operating Manual (NISPOM). When visiting COMSPAWARSYSCOM at either the Old Town Campus (OTC) or Point Loma Campus (PLC) the Contractor will comply with 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 Commander SPAWAR Systems Command (COMSPAWARSYSCOM's) Security Contracting Officer's Representative (COR), Code D0355. If the Contractor establishes a cleared facility or Defense Security Service (DSS) approved off-site location at COMSPAWARSYSCOM, the security provisions of the NISPOM will be followed within this cleared facility.

b. Security Supervision. SPAWAR SYSTEMS CENTER SAN DIEGO will exercise security supervision over all contractors visiting COMSPAWARSYSCOM and will provide security support to the Contractor as noted below. The Contractor will identify, in writing to the Security's COR, an on-site Point of Contact to interface with the Security's COR.

II. HANDLING CLASSIFIED MATERIAL OR INFORMATION.

a. Control and Safeguarding. Contractor personnel located at COMSPAWARSYSCOM 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 SAN DIEGO conducted Security Briefings, available at this time by appointment only. In the event of possible or actual loss or compromise of classified material, the on-site Contractor at the OTC will immediately report the incident to SPAWAR SYSTEMS CENTER SAN DIEGO's Code D0355 as well as the Contractor's FSO. An on-site Contractor, whose primary location is OTC, will make their report to Code D0355 as well as the Contractor's FSO. A Code D0355 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 the SPAWAR SYSTEMS CENTER SAN DIEGO representative.

b. Storage.

1. Classified material may be stored in containers authorized by SPAWAR SYSTEMS CENTER SAN DIEGO's PLC Physical Security Group, Code D0354, or OTC Code D0355 for the storage of that level of classified material. Classified material may also be stored in Contractor owned containers brought on board COMSPAWARSYSCOM with Code D0354's written permission. Containers to be located at our OTC will request Code D0355's written permission. Areas located within cleared contractor facilities at COMSPAWARSYSCOM will be approved by DSS.

2. The use of Open Storage areas must be pre-approved in writing by Code D0353 for PLC, or Code D0355 for OTC, 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 SAN DIEGO, Code D0353 for PLC or Code D0355 for the OTC.

c. Transmission of Classified Material.

1. All classified material transmitted by mail for use by long term visitors will be addressed to COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND, 4301 PACIFIC HIGHWAY, 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 COMSPAWARSYSCOM PLC by contractor personnel must be delivered to the Classified Material Control Center (CMCC), Code D0351, for processing.

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

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

5. The sole exception to the above are items categorized as a Data Deliverable. All contract Data Deliverables will be addressed to the location listed 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 COMSPAWARSYSCOM 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 COMSPAWARSYSCOM will be considered long term visitors for the purpose of this contract.

b. Submission of valid Visit Authorization Letter (VAL) for classified access to COMSPAWARSYSCOM is the responsibility of the Contractor's Security Office. All VAL's will be prepared in accordance with the NISPOM. They will be mailed to COMMANDING OFFICER, ATTN CODE D03541, SPAWAR SYSTEMS CENTER, 49275 ELECTRON DRIVE, SAN DIEGO, CA 92152-5435 for the PLC, or COMMANDING OFFICER, VISITOR CONTROL OTC, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, SAN DIEGO, CA 92152-5001 for OTC. The VAL's will be addressed to COMSPAWARSYSCOM and list a COMSPAWARSYSCOM point of contact. Visit requests may be sent via facsimile to the PLC at (619) 553-6169, and verified on 553-3203 or the OTC at (619) 524-2745, and verified on (619)524-2751 or (619)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 D03541 for PLC or OTC, will issue temporary identification badges to Contractor personnel following receipt of a valid VAL from the Contractor's FSO. The responsible COMSPAWARSYSCOM COR will request issuance of picture badges to contractor personnel. The COR may, at their discretion, request that picture badges be issued for the length of the basic contract or option period. Identification badges are the property of the U.S. Government and will be worn and used for official business only. Unauthorized use of an COMSPAWARSYSCOM badge will be reported to the DSS. Identification badges must be worn in plain sight at all times on board COMSPAWARSYSCOM.

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

1. Notify in writing Code D03541 for PLC, Code D0355 for OTC, the COR, the Security's COR and the laboratory managers of any laboratories into which the employee had been granted unescorted access of the

termination and effective date. In emergency situations, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.

2. Confiscate any COMSPAWARSYSCOM identification badge and vehicle decal and return them to either Code D03541 (PTL), or Code D0355 (OTC), no later than 5 working days after the effective date of the termination.

V. INSPECTIONS. Code D0355 personnel will conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel will cooperate with Code D0355 representatives during these inspections. All contractor personnel will cooperate with Code D0355 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 D0355 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 the Security's COR, Code D0355. This reporting will include the following:

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

#### VII. PHYSICAL SECURITY.

a. SPAWAR SYSTEMS CENTER SAN DIEGO will provide appropriate response to emergencies occurring onboard this Division. The Contractor will comply with all emergency rules and procedures established for COMSPAWARSYSCOM.

b. A roving Contract Security Guard patrol will be accomplished by SPAWAR SYSTEMS CENTER SAN DIEGO. Such coverage will consist of, but not be limited to, physical checks of the window or door access points, classified containers, and improperly secured documents or spaces. Specific questions or concerns should be addressed to either PLC Code D0354 or OTC Code D0355.

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

#### VIII. FOREIGN TRAVEL

a. Contractor must ensure that, prior to all foreign travel under this contract, personnel receive a Force Protection/Anti-Terrorism briefing. The online briefings are available at the following URL:

<http://iweb.spawar.navy.mil/services/security/training/antitersd/brief.html> .

Those without access to the intranet can use the following URL:

<http://www.spawar.navy.mil/sandiego/security/FP-AT/antiterror.html>

For contractor personnel outside San Diego, information regarding briefing available may be obtained from a local Naval Criminal Investigative Service Office.

b. Aforementioned briefings expire after six months and must be repeated prior to additional foreign travel. Area-specific briefings are required for travel to areas designed as medium to critical threats. OTC Code D0355 personnel may be contacted for current threat level information and area-specific briefings

#### IX. 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 submits a Final DD254 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 when required.

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

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

#### XI. ITEMS PROHIBITED ABOARD COMSPAWARSYSCOM.

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

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

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

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

poison, acids or caustic chemicals;

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

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

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

## XII. ESCORTING POLICY.

a. All personnel within COMSPAWARSYSCOM's fenced perimeters, with the exception of emergency personnel such as fire, ambulance, or hazardous material response personnel responding to an actual emergency, must wear a COMSPAWARSYSCEN issued badge. The words "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 intending citizens (Former immigrant aliens) may be escorted under this policy. ALL FOREIGN NATIONAL VISITORS MUST BE PROCESSED THROUGH THE COMSPAWARSYSCOM FOREIGN DISCLOSURE OFFICE.

b. All permanently badged COMSPAWARSYSCOM and tenant command employees, as well as those contractors and other government employees who have an "E" on their red and blue, respectively backgrounded permanent badges may escort those visitors requiring an escort-required badge. An "E" on the badge of a contractor employees DOES NOT PERMIT ESCORTING OF FOREIGN NATIONAL VISITORS.

**ELECTRONIC DATA SYSTEMS CORPORATION**  
**N00024-00-D-6000**  
**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 THE 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.

**ELECTRONIC DATA SYSTEMS CORPORATION**  
**N00024-00-D-6000**  
**AUTOMATED INFORMATION SYSTEM (AIS) PERSONNEL SECURITY PROGRAM REQUIREMENTS**

The U.S. Government conducts trustworthiness investigations of personnel who require access to only Unclassified information and who perform AIS 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>. Falsification of information submitted for any government-conducted investigation may result in contract default. The contractor shall include all of these requirements in any subcontracts involving AIS support.

Personnel performing work on AIS may be either a U.S. citizen or an Immigrant Alien (except as noted below). An Immigrant Alien is defined as a foreign national lawfully admitted to the United States for permanent residence. These personnel shall be designated as filling one of the three AIS Categories listed below. The Contracting Officer's Representative (COR) or Technical Representative (TR) shall determine if they or the contractor shall assign the AIS 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.

**AIS Category I (High Risk)** – may be filled by U.S. citizens only. 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 AIS Category I designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR), the updated standard for the BI listed in DoD 5200.2-R. The SSBI or SSBI-PR shall be updated every 5 years.

**AIS Category II (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 AIS Category I level to insure the integrity of the system. Personnel whose duties meet the criteria for an AIS Category II designation require a favorably adjudicated National Agency Check (NAC), instead of the DNACI/NACI listed in DoD 5200.2-R.

**AIS Category III** - all other positions. Personnel whose duties meet the criteria for an AIS Category III 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 AIS Category I is less than 5 years old, you do not need to submit an additional Electronic Personnel Security Questionnaire (EPSQ) for the trustworthiness determination. If required, the contractor will ensure personnel designated AIS category I, II, or III complete the EPSQ Standard Form (SF) 85P and provide it to their company's designated reviewer for an initial suitability determination. The reviewer will use the criteria outlined in Appendix G, SECNAVINST 5510.30A to make this initial determination. If, based on this initial review, the contractor gives the employee a negative trustworthiness determination the contractor will identify a replacement to the COR or TR and direct the replacement to complete the EPSQ. For personnel the contractor deems suitable, the designated reviewer will submit their EPSQs to DSS. Investigative packages shall be submitted for all personnel in AIS Category I, II, or III prior to the employee being granted access to the AIS. Specific guidelines for obtaining software and submission of EPSQs are available at the Defense Security Service (DSS) Internet Web Site. If you are unfamiliar with the EPSQ SF85P, you may contact your local DSS Office for further information.

Investigation results shall be returned to SPAWARSSYSCEN San Diego, Code D0352, 53560 Hull Street, San Diego, CA 92152-5001 for a trustworthiness determination. SPAWARSSYSCEN San Diego will notify the contractor of its decision. The contractor will promptly replace any individual for whom SPAWARSSYSCEN San Diego has communicated a negative trustworthiness determination.

The contractor will include the AIS Category for each person so designated on Visit Authorization Letters (VAL). VALs will be sent to the following address: Commanding Officer, SPAWARSSYSCEN San Diego, ATTN: Code D03541, 49275 Electron Drive, San Diego, CA 92152-5435.

**ELECTRONIC DATA SYSTEMS CORPORATION  
FOR OFFICIAL USE ONLY (FOUO) INFORMATION  
N00024-00-D-6000**

1. The For Official User 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.
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 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" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back cover, and on the outside of the back cover (if any). No portion markings will be shown.
4. Within a classified document, an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked, "FOUO."
5. Any FOUO information released to you by COMSPAWARSYSCOM is required to be marked with the following statement prior to transfer:  
  
THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS \_\_\_\_ 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 COMSPAWARSYSCOM 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 container or in the uncontrolled burn.
11. Unauthorized disclosure of FOUO information doesn't constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

**TEMPEST REQUIREMENTS QUESTIONNAIRE  
FOR CONTRACTOR FACILITIES  
CONTRACT NO: N00024-00-D-6000**

1. This TEMPEST Requirements Questionnaire (TRQ) must be completed and sent to the contracting authority and the Certified TEMPEST Technical Authority (CTTA) within 30 days after contract award for all contracts where classified National Security Information (NSI) will be processed and the requirements of item 13 of the DD Form 254 have been met.
2. The prime contractor cannot pass TEMPEST requirements to subcontractors. Subcontractors must submit a Contractor TRQ prior to processing.
3. The TRQ is for information collection only. It is not a directive or an implied requirement, nor is it an encouragement to procure TEMPEST equipment or any type of shielding for use on this contract. Do not initiate any changes to equipment of facilities for TEMPEST unless it has been recommended by the CTTA and specifically directed by the contracting authority.
4. The contracting authority will not issue any directives concerning TEMPEST until after the contractor submitted TRQ has been evaluated by the CTTA and resulting recommendations received. To fully evaluate the TRQ, the CTTA may request additional information concerning the facility, its physical control, the equipment which will be used to process NSI, etc.
5. The contractor shall ensure compliance with any TEMPEST countermeasure(s) specifically directed in writing by the contracting authority.
6. Please provide the information requested in paragraphs 7 through 20 and return to the contracting authority identified in item 16 of the DD Form 254 and to the CTTA at:

Commanding Officer  
SPAWARSYSCEN Charleston  
Code 723  
PO Box 190022  
North Charleston, SC 29419-9022

7. Provide the name, address, position title and phone number (at the facility where classified processing will occur) of a point of contact who is knowledgeable of the processing requirements, the types of equipment to be used and the physical layout of the facility.
8. Provide the specific geographical location, address, and zip code, where classified processing will be performed.
9. What are the classification level(s) of material to be processed/handled by electronic or electromechanical information system(s) and what percentage is processed at each level?
10. What special categories of classified information are processed?
11. Is there a direct connection (wireline or fiber) to a Radio Frequency (RF) transmitter(s) located either locally or at a remote site?
12. Are there any RF transmitters located within 6 meters of the system processing National Security Information or the system's RED signal lines?

**BLOCK 13 ACCESS REQUIREMENTS CONTINUED:**

11.G THE CONTRACTOR IS AUTHORIZED THE USE OF DTIC REGARDING CONTRACT RELATED MATTER AND WILL PREPARE AND PROCESS DD FORM 1540 IN ACCORDANCE WITH THE NISPOM, CHAPTER 11, SECTION 2. THE COR WILL CERTIFY NEED-TO-KNOW TO DTIC.

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

11L. CLASSIFIED AIS PROCESSING SHALL BE IN ACCORDANCE WITH THE PROVISIONS OF THE NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM), CHAPTER 8, AND MUST BE PERFORMED ON AN ACCREDITED COMPUTER SYSTEMS APPROVED BY DSS.

VISIT REQUESTS TO OTHER THAN COMSPAWARSYS COM SHALL HAVE "NEED TO KNOW" CERTIFIED BY TECHNICAL REPRESENTATIVE, PMW 164-4.

13. Describe how access is controlled to your facility including the building, compound, plant, property, and/or parking lots. Where are visitor's first challenged/identified? Include controls such as alarms, guards, patrols, fences and warning signs. Provide a simple block diagram of the equipment, the facility and the surrounding areas. The diagram(s) should extend out to the nearest uncontrolled area on each side of the facility, such as a military base perimeter, plant property line, commercial building or residential area.
14. Are there other tenants in the building who are not U.S. department/agencies or their agents?
15. Are there any known foreign business or government offices in adjacent buildings?
16. Provide the make and model number of all equipment used to process, transfer or store classified information. Include computers, peripherals, network servers, network hardware, multiplexers, modems, encryption devices (COMSEC), etc.
17. Have on-site TEMPEST tests been conducted on any of these equipment(s)? If so, which ones? When was the test(s) conducted? Who conducted the test(s)? Have all deficiencies (if any) been resolved?
18. Has a TEMPEST Facility Zoning test been conducted? If so, who conducted the testing and when?
19. Is this company foreign-owned or controlled? If so, what is the country?
20. Provide the name, code, telephone number, and address of the Contracting Officer's Representative, the contract number and the sponsoring command.

4/98 TRQcntr.DOC