AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT	1. CONTRACT ID CODE	PAGE OF PAGES 1 / 1

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
P00071	SEE BLOCK 16C		

6. ISSUED BY CODE N00039

COMMANDER
SPACE AND NAVAL WARFARE SYSTEMS COMMAND
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127
Joel Judy, 02-21M (619) 524-7179, joel.judy@navy.mil

7. ADMINISTERED BY (If other than Item 6) CODE S5111A

DCMA-SOUTHERN VIRGINIA
190 BERNARD ROAD, BLDG. 117
FORT MONROE, VA 23651

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State, and ZIP Code)

AVAYA INC.
211 MOUNT AIRY ROAD, ROOM 1C316
BASKING RIDGE, NJ 07920-2336

For administrative purposes, all contractual correspondence and orders are to be directed to Avaya Inc., 5440 Millstream Road, McLeansville, NC 27301, Cage Code 1SBH3.

CODE 1RHB2 FACILITY CODE

(✓) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO. N68939-97-D-0040

✓ 10B. DATED (SEE ITEM 13) 29 July 1997

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; of (c) By separate letter of telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT 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)

To Be Specified on the Individual Delivery Orders

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.
IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

(✓) A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A. (Specify authority) THE CHANGES

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b)

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

X D. OTHER
MUTUAL AGREEMENT OF THE PARTIES

E. IMPORTANT: Contractor __ is not X is required to sign this document and return 1 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 incorporate an updated DD Form 254 Contract Security Classification Specification into the basic contract (See Attachment 1). All other terms and conditions of contract N68939-97-D-0040 shall remain unchanged and in full force and effect.

This modification constitutes the entire understanding between the parties and supercedes the terms and conditions of all other prior or contemporaneous oral or written agreements between the parties. Failure by either party to enforce any of the provisions of this modification shall not be construed as a waiver by such party of any such provisions, nor shall such failure affect the validity and enforceability of this modification in any way.

15A. NAME AND TITLE OF SIGNER (Type of print):		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or Print)	
J.K. Sheek, RCM		CARLA J. BROWN	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED 16 Dec 2004	16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C. DATE SIGNED 12/16/04

NSN 7540-01-152-8070
PREVIOUS EDITION UNUSABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 DFR) 53.243

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
TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED
NONE

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

X	a. PRIME CONTRACT NUMBER N68939-97-D-0040	
	b. SUBCONTRACT NUMBER	
	c. SOLICITATION OR OTHER NUMBER	DUE DATE *(YYYYMMDD)*

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

	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)* 19970729
X	b. REVISED *(Supersedes all previous specs)*	REVISION NO. 6	DATE *(YYYYMMDD)* 20041207
	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)*
AVAYA INC. 211 MOUNT AIRY ROAD, ROOM 1C316 BASKING RIDGE, NJ 07920-2336	1RHB2	DEFENSE SECURITY SERVICE (DSS) TWO GREENTREE CENTRE, SUITE 120 MARLTON, NJ 08053-3102

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

VOICE, VIDEO AND DATA (VIVID)

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) REFER TO REMARKS IN BLOCK 13	X	
k. OTHER (Specify) PR NO.:		X			

PR NO.: CONTRACT NUMBER: N68939-97-D-0040 (REV. 6)

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)*: **RELEASE OF COMSEC INFORMATION IS NOT AUTHORIZED.**

COMMANDER, SPACE AND NAVAL WARFARE SYSTEMS COMMAND (SPAWARSYSCOM), CODE 00L, 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 (CONTINUE ON NEXT PAGE):

10.A FURTHER DISCLOSURE, TO INCLUDE SUBCONTRACTING, OF COMSEC INFORMATION BY A CONTRACTOR REQUIRES PRIOR APPROVAL OF THE SPAWAR SYSTEMS CENTER TECHNICAL POINT-OF-CONTACT, CODE 2829. ACCESS TO ANY COMSEC INFORMATION REQUIRES SPECIAL BRIEFINGS A THE CONTRACTOR'S FACILITY. ACCESS TO CLASSIFIED COMSEC INFORMATION REQUIRES A FINAL U.S. GOVERNMENT CLEARANCE AT THE APPROPRIATE LEVEL.

10.J 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/HTML/52001R.HTM.

11.A CONTRACT PERFORMANCE IS RESTRICTED TO DESIGNATED NAVY, AIR FORCE, ARMY, DEFENSE LOGISTIC AGENCIES AND DEFENSE COMMUNICATIONS AGENCIES LOCATIONS. DETAILS REGARDING SPECIFIC WORK PERFORMANCE LOCATIONS WILL BE PROVIDED IN EACH DELIVERY ORDER. THE SPAWAR SYSTEMS CENTER TECHNICAL POINT-OF-CONTACT, CODE 2829, WILL PROVIDE SECURITY CLASSIFICATION GUIDANCE AS NEEDED FOR PERFORMANCE OF THIS CONTRACT.

NOTE: THIS CONTRACTOR HAS NO CLASSIFIED STORAGE APPROVAL AT THIS TIME. ANY CLASSIFIED MATERIAL ACCESSED BY THIS CONTRACTOR MUST BE STORED AT THE HOST U.S. GOVERNMENT ACTIVITY.

THE SPAWAR SYSTEMS CENTER TECHNICAL POINT OF CONTACT IS MR. TED G. WOLKEN, CODE 2829, (619) 524-9601; EMAIL: TED.WOLKEN@NAVY.MIL; MAILING ADDRESS: COMMANDING OFFICER, SPAWAR SYSTEMS CENTER, CODE 2829, 53560 HULL STREET, SAN DIEGO, CA 92152-5001.

VISIT REQUESTS TO OTHER THAN **SPAWAR SYSTEMS CENTER** SHALL HAVE "NEED TO KNOW" CERTIFIED BY CODE 2829.

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 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.)

ATTACHMENT (1): INFORMATION TECHNOLOGY SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS AND MUST BE PROVIDED TO ALL SUBCONTRACTORS REQUIRING ACCESS TO U.S. GOVERNMENT OWNED OR U.S. GOVERNMENT MANAGED IT SYSTEMS.

ATTACHMENT (2): SPECIFIC ON-SITE SECURITY REQUIREMENTS FOR SPAWAR SYSTEMS CENTER. FOR AUTHORIZED VISITS TO OTHER U.S. GOVERNMENT ACTIVITIES, THE CONTRACTOR MUST COMPLY WITH ALL ON-SITE SECURITY REQUIREMENTS OF THE HOST COMMAND.

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)*
SUSAN VILLARREAL SUE.VILLARREAL@NAVY.MIL	SECURITY'S CONTRACTING OFFICER'S REPRESENTATIVE (COR)	(619) 524–2672

d. ADDRESS *(Include Zip Code)*

COMMANDING OFFICER
SPAWAR SYSTEMS CENTER, CODE 20351
53560 HULL ST.
SAN DIEGO, CA 92152-5001

e. SIGNATURE

20041207 Susan M. Villarreal

17. REQUIRED DISTRIBUTION

☒ a. CONTRACTOR
☐ b. SUBCONTRACTOR
☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AN D SUBCONTRACTOR
☒ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
☒ e. ADMINISTRATIVE CONTRACTING OFFICER CODE
☒ f. OTHERS AS NECESSARY: SPAWAR SYSTEMS CENTER, CODE 20351, ATTN: SUE VILLARREAL; AND SPAWAR SYSTEMS CENTER, CODE 2829, ATTN: TED WOLKEN

BLOCK 13, ACCESS REQUIREMENTS CONTINUE:

11.E CONTRACT IS FOR EQUIPMENT MAINTENANCE SERVICES ON EQUIPMENT PROCESSING CLASSIFIED INFORMATION. ACTUAL KNOWLEDGE OF, GENERATION OR PRODUCTION OF CLASSIFIED INFORMATION IS NOT REQUIRED FOR PERFORMANCE OF THIS CONTRACT. CLEARED PERSONNEL ARE REQUIRED TO PERFORM SERVICES FOR THOSE SITES WHERE CLASSIFIED ACCESS CANNOT BE PRECLUDED BY ESCORTING AND SANITIZATION BY SITE PERSONNEL.

11.F ACCESS TO CLASSIFIED U.S. GOVERNMENT INFORMATION MAY BE REQUIRED AT THE FOLLOWING OVERSEAS U.S. GOVERNMENT LOCATIONS: ENGLAND, SPAIN, ITALY, SINGAPORE, JAPAN/OKINAWA; VARIOUS HOST SITES WITHIN MIDDLE EASTERN COUNTRIES; AND POSSIBLY OTHER LOCATIONS, AS DEEMED APPROPRIATE. THE EXACT DESTINATIONS WILL BE LISTED IN EACH DELIVERY ORDER.

ANTI –TERRORISM / FORCE PROTECTION BRIEFINGS ARE REQUIRED FOR PERSONNEL PRIOR TO COMMENCEMENT OF FOREIGN TRAVEL.

11.K THE SPAWAR SYSTEMS CENTER TECHNICAL POINT-OF-CONTACT, CODE 2829, APPROVES AUTHORIZATION FOR CONTACTOR TO HAVE A DEFENSE COURIER SERVICE (DCS) ACCOUNT WITH PRIOR VALIDATION. THE CONTRACTOR SHALL MAKE ARRANGEMENTS TO USE THE SERVICES OF THE DCS FOR TRANSPORTATION OF QUALIFIED MATERIAL.

11.L CLASSIFIED INFORMATION TECHNOLOGY (COMPUTER) PROCESSING (ASHORE) 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. ALL CLASSIFIED IT PROCESSING ABOARD US FLAG OR FOREIGN FLAG VESSELS SHALL BE IN ACCORDANCE WITH SECNAVINST 5510.36 AND SECNAVINST 5239.3. **ALL TECHNICIANS AS WELL AS ANY OTHER CONTRACTOR PERSONNEL REQUIRING ACCESS TO IT GOVERNMENT SYSTEMS MUST BE U.S. CITIZENS AND MEET THE SECURITY CLEARANCE ACCESS REQUIREMENTS OF THE SITE.**

NO FURTHER ENTRIES ON THIS PAGE.

INFORMATION TECHNOLOGY (IT) SYSTEMS PERSONNEL SECURITY PROGRAM REQUIREMENTS – Attachment 1

Authority/Purpose:

The U.S. Government conducts trustworthiness investigations of personnel who are assigned to positions that directly or indirectly affect the operation of unclassified information technology (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), Investigations Service (IS), Federal Investigations Processing Center (FIPC) has been delegated authority to 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/html/52002r.htm. 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 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.

DoD 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." 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 C 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 (High Risk)

- Responsibility or the development and administration of Government computer security programs, and also 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 SPAWARSYSCEN San Diego CA 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.

IT-II Position (Moderate Risk)

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 SPAWARSYSCEN San Diego CA that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in IT -I positions. Personnel whose duties meet the criteria for an IT -II Position require a favorably adjudicated National Agency Check (NAC).

IT -III Position (Low Risk) -

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

Qualified Cleared Personnel Do NOT Require Trustworthiness Investigations:

If an employee is in a position that **does not** require a personnel security clearance, **do not** submit a request for clearance, simply submit the Public Trust Position Application, Standard Form (SF) 85P, for trustworthiness determination. If an employee has already been granted a personnel security clearance at the appropriate level without a break in service for more than 24 months, and in the case of IT -I Position has had a completed Personnel Security Investigation (a Single Scope Background Investigation-SSBI) less than 5 years old, you do **not** need to submit an additional investigation for the trustworthiness determination.

Procedures for submitting U.S. Government Trustworthiness Investigations:

The contractor will ensure personnel designated IT -I, II, or III complete either the hard copy SF 85P *or* the online—electronic (Electronic Personnel Security Questionnaire—EPSQ) version of the SF85P. Instructions on where to obtain and how to complete the SF85P are found below.

The investigative request package for the SF85P from the OPM web site (non-EPSQ) version consists of the following: 1) Completed and Validated Error-free SF85P; 2) OPM Fingerprint Card FD 258; 3) Security Officer's portion of the SF85P; 4) signed Privacy Act release (to include a signed Medical release, when applicable); and 5) in the "Your Employment Activities" block add the contract number requiring the Trustworthiness Investigation. Note: Do not complete a separate OPM coversheet if using this SF85P form. The SF85P is available from OPM at http://www.opm.gov/forms/html/sf.asp with additional assistance at http://www.dss.mil/.

When using the SF85P--EPSQ version, the submitted package shall include: 1) A hard copy of the SF85P; 2) all pertinent signed release forms; 3) OPM Fingerprint Card FD 258; 4) Employee's and Security Officer's validation certificates; 5) an OPM coversheet signed and dated by the employee and FSO; and 6) in the "Your Employm ent Activities" block add the contract number requiring the Trustworthiness Investigation. The FSO is responsible for completing the OPM coversheet that is available for downloading with instructions at: http://www.opm.gov/extra/investigate/dodsf85.pdf. Note: For item "J" on this coversheet, use your company's Submitting Office Number (SON). If this is not available, contact OPM -FIPC Program Services Office (PSO) to apply for a SON by calling 724.794.5612. For item " L" insert "N030". Then for item "N" enter "DSS-IND".

The company shall review the SF85P for completeness and use SECNAVINST 5510.30A, Appendix G available at http://neds.nebt.daps.mil/551030.htm to determine if any adverse information is present. ***Only hard copy SF85Ps are acceptable by OPM-FIPC***. Additional guidance for requesting investigations from OPM is found at http://www.opm.gov/extra/investigate/IS-15.pdf. Completed SF85P packages will be mailed to: OPM-FIPC, P.O. Box 618, Boyers, PA, 16018-0618. Note: All forms must be signed within 120 days of the date of submission to OPM. Submitted forms, which are not received within these 120 days, will be delayed or returned. If no change has occurred, forms must be re-dated and initialed by the Subject/employee.

If you require additional assistance for SF85P or related concerns, you may send email to SPAWARSYSCEN San Diego CA at SF85P@spawar.navy.mil.

Visit Authorization Letters (VALs) for Qualified Employees:

The contractor will include the IT Position Category for each person so designated on a VAL once the COR or TR has approved the Category. VALs will be sent to the following address: Commanding Officer, SPAWARSYSCEN San Diego, ATTN: Code 20352, 49275 Electron Drive, San Diego, CA 92152-5435.

Employment Terminations:

The contractor shall:

- Immediately notify the COR or TR of the employee's termination;
- Send email to SF85P@spawar.navy.mil.
- Fax a termination VAL to Code 20352 at (619) 553-6169.
- Return any badge and decal to Code 20352.

If an individual received a negative trustworthiness determination, they will be immediately removed from their position of trust, the contractor will follow the same employee termination processing above, and they will replace any individual who has received a negative trustworthiness determination.

SPECIFIC ON-SITE SECURITY REQUIREMENTS - Attachment 2

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 controlled unclassified information, SECNAVINST 5510.36 (series), SECNAVINST 5510.30 (series), and NRADINST 5720.1(series). Both of the SECNAV Instructions are available online at http://neds.nebt.daps.mil/directives/table52.html. A copy of NRADINST 5720.1 will be provided upon receipt of a written request from the Contractor's Facility Security Officer (FSO) to the SPAWAR Systems Center Security's Contracting Officer's Representative (COR), Code 20351. 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 20351, telephone (619) 553-0437, as well as the Contractor's FSO. A Code 20351 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 20352 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 20352'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 20352 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 20352.

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 (SCI) material using the Defense Courier Service: SPAWARSYSCEN-SAN DIEGO: 271582-SN00, SPAWARSYSCEN SAN DIEGO.

(b) CONFIDENTIAL and SECRET material transmitted by FedEx, USPS Registered, Express mail will be addressed to COMMANDING OFFICER, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, SAN DIEGO CA 92152-5001. The inner envelope will be addressed to the attention of the Contracting Officer's Representative (COR) or applicable Technical Representative (TR) for this contract, to include their code number.

2. All SECRET material hand carried to SPAWAR Systems Center by contractor personnel must be delivered to the Classified Material Control Center (CMCC), Code 20332, building 33, room 1305, for processing.

3. All CONFIDENTIAL material hand carried to SPAWAR Systems Center by contractor personnel must be delivered to the Mail Distribution Center, Code 20331, 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 2206, SPAWAR SYSTEMS CENTER, 53560 HULL STREET, 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 20352, 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 one year.

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 20352 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, will be worn in plain sight, and used for official business only. Unauthorized use of an SPAWAR Systems Center badge will be reported to the DSS.

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 20352, 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 emergencies, a facsimile may be sent or a telephone notification may be used. The telephone notification, however, must be followed up in writing within five working days.

2. Immediately confiscate any SPAWAR Systems Center issued identification badge and vehicle decal and return them to Code 20352 no later than five working days after the effective date of the termination.

V. INSPECTIONS. Code 20351 personnel may conduct periodic inspections of the security practices of the on-site Contractor. All contractor personnel will cooperate with Code 20351 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 20351 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 20351. If further investigation is warranted it will be conducted by Code 20351. This reporting will include the following:

a. The denial, suspension, or revocation of security clearance of any assigned personnel;

b. Any adverse information 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 command. The Contractor will comply with all emergency rules and procedures established for SPAWAR Systems Center.

b. A roving Contract Security Guard patrol will be provided 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 20352.

c. All personnel aboard SPAWAR Systems Center are subject to random inspections of their vehicles, personal items and of themselves. Consent to these inspections is given when personnel accept either a badge or a vehicle pass/decal permitting entrance to this command.

d. Information about parking restrictions may be found on the Security web site at https://iweb.spawar.navy.mil/services/security/html/Parking.html.

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 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 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 SPAWAR SYSTEMS CENTER.

The following items are prohibited within any SSC San Diego controlled areas, with the exception of personnel authorized to possess weapons in the performance of required duties.

If an individual is attempting entry onto SSC San Diego controlled spaces and discloses the possession of a weapon prior to being instructed to comply with an administrative weapons inspection, the gate guard or inspection team will deny base entry to that individual and will report the circumstances to the SSC San Diego Security Officer. If the disclosure of a firearm, explosive or dangerous weapon is made during the inspection or if no disclosure is made at all, the individual will be detained and the SUBASE Precinct will be notified.

WEAPONS

a. Ammunition.
b. Fireworks.
c. Molotov Cocktail.
d. Pipe Bomb.
e. Black Jack.
f. Slingshots.
g. Billy/Sand Club.
h. Nunchakus.
i. Sand Bag: Partially filled with sand and swung like a mace.
j. Metal (Brass) Knuckle.
k. Dirk or Dagger.
l. Switch Blade or Butterfly Knife.
m. Knife with a blade (cutting edge) longer than 4 inches. NOTE: this represents a change from the previous 2.5-inch limit.
n. Razor with Unguarded blade.
o. Pipe, Bar or Mallet to be used as a club.
p. Compressed Air or Spring Fired Pellet/BB gun.
q. Tear Gas/Pepper Spray Weapon.
r. Pistol, Revolver, Rifle, Shotgun or any other Firearm.
s. Bows, Crossbows, or Arrows.
t. Bowie Style Hunting Knife.
u. Any weapon prohibited by State law.
v. Any object similar to the aforementioned items.
w. Any offensive or defensive weapons not described above, but likely to cause injury (i.e., Stun Gun, Blow Gun).
x. Any abrasive, caustic, acid, chemical agent, or similar substance, with which to inflict property damage or personal injury.
y. Combination Tools with Knife Blades Longer Than 4 inches (i.e., Gerber, Leatherman, etc.).

Military personnel aboard SSC SD 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

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

Permission to possess and consume alcohol on-site at SSC San Diego is at the exclusive discretion of the Commanding Officer. That includes the determinations of where and when alcohol may be brought on board the Center and consumed. SSC San Diego personnel 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.

Open containers of any alcoholic beverage unless for use at a function approved by the SSC San Diego Commanding Officer. Employees desiring to hold a function and serve alcohol, should send a memo (hard copy) to the Commanding Officer, via the appropriate division head, the Director of Security, and the Public Affairs Officer. The Public Affairs Officer will approve or disapprove the facility use request based on availability and general use policy. If facility use is approved, the Public Affairs Officer will forward the memo to the Commanding Officer for approval/disapproval. Manufacturer sealed containers of alcoholic beverage are authorized as long as the containers remain sealed while within SSC San Diego controlled spaces. Further information is available at https://iweb.spawar.navy.mil/services/security/docs/letteralcohol.doc.

COUNTERFEIT CURRENCY

Counterfeit currency defined as any copy, photo, or other likeness of any U.S. currency, either past or present, not authorized by the U.S. Treasury Department is prohibited.

XI. ESCORTING POLICY.

a. All personnel within 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. Code 2035 or Code 2038 employee's with badges displaying the word "Security" or "Safety" 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, CODE 20351.

b. All pictured badged SPAWAR Systems Center and tenant command employees, as well as those contractors and other government employees who have an "E" on their picture badge may escort visitors wearing a red escort-required badge.