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
TOP SECRET

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

☒	a. PRIME CONTRACT NUMBER N00244-16-D-00XX	
☐	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*) 20160801
☐	b. REVISED (Supersedes all previous specs)	Revision No.	DATE (*YYYYMMDD*)
☐	c. FINAL (*Complete item 5 in all cases*)		DATE (*YYYYMMDD*)

4. IS THIS A FOLLOW-ON CONTRACT? ☒ YES ☐ NO. If yes, complete the following:

Classified material received or generated under N00244-08-D-0036 (*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 Code*)

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

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

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

On-Orbit Engineering Support (OOES)

10. THIS CONTRACT 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 ONLYINFORMATION	X		l. OTHER (*Specify*)		
k. OTHER (*Specify*)					

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*): Commanding Officer, Naval Satellite Operations Center

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.)

SECNAVINST 5510.30B Department of the Navy (DON) Personnel Security Program (PSP) Instruction, 6 Oct 2006
SECNAVINST 5239.3B Department of the Navy Information Assurance Policy, 17 Jun 2009
NAVSOCINST 5234.1B Automated Information Security (AIS) Software Control, 12 Jun 2002
NAVSOCINST 5530.1A, Physical Security and Loss Prevention Plan, 09 Mar 1998
SECNAVINST 5510.36A Department of the Navy (DON) Information Security Program (ISP), 06 Oct 2006
DOD 5220.22-M, National Industrial Security Program Operating Manual, 28 Feb 2006
Global Broadcast Service Security Classification/Declassification Guide dated 29 April 2007
OPNAVINST 5513.6D OF July 21, 2008
Security Classification Guidance for FLTSATCOM Anomalies dated 20 April 1993
NAVSOC Contractor Security Guidance
National Security Agency Central Security Service NSA/CSS Policy Manual No. 3-16 dated 05 August 2005

Reference Block 10a: COMMUNICATIONS SECURITY (COMSEC) INFORMATION - Access to COMSEC information is restricted to those employees who are U.S citizens holding a government-issued final security clearance at the appropriate level, and who have been briefed according to the DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), and National Security Agency Central Services NSA/CSS Policy Manual No. 3-16. However, an Interim Top Secret clearance is valid for access to COMSEC at the Secret and Confidential levels.

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.*) ☐ YES ☒ NO

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. (*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.*) ☐ YES ☒ NO

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*)
PAUL LAGANA	Security Manager	805-989-4210

d. ADDRESS (*Include Zip Code*)	17. REQUIRED DISTRIBUTION	
661 13th Street Point Mugu, CA 93042	X	a. CONTRACTOR
		b. SUBCONTRACTOR
	X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE		d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
		e. ADMINISTRATIVE CONTRACTING OFFICER
	X	f. OTHERS AS NECESSARY

NAVSOC On-Site Contractor Security Guidance
Attachment #1 to DD Form 254 For Contract # N00244-XX-X-XXXX

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 to the requirements of DoD 5220.22-M, Department of Defense National Industrial Security Program Operating Manual (NISPOM).

Additionally, when visiting or working at NAVSOC facilities, Contractor personnel will comply with the Host Installation and NAVSOC Security Directives relative to security policies and procedures as they apply to the protection of classified and controlled but unclassified information. If the contractor establishes a cleared facility or Defense Security Service approved off-site location in support of this contract the security provisions of the NISPOM alone will apply to that facility.

b. Identification Requirements. All contractor personnel performing under this statement of work shall identify themselves as a contractor employee to avoid creating any impression that they are Government officials. Such identification shall be made in all meetings attended, when answering Government telephones, on all e-mails, and when working in other situations where their contractor status is not obvious to third parties. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

c. Security Supervision. NAVSOC will exercise security oversight over all contractors visiting or working at NAVSOC Facilities. The contractor will identify, in writing, to the NAVSOC Security Manager (or designated detachment security representative), an on-site management Point of Contact (POC) that will interface with the NAVSOC Security Manager for security matters.

d. Company Facility Security Officer (FSO). The contractor shall provide the NAVSOC Security Manager, in writing, the name, address, telephone number, and email address of the Company's cognizant FSO. The contractor shall ensure that these names and addresses are kept current. The FSO will report any change in status of company employees such as clearance level, name change, resignation, foreign contacts, etc. to the Personnel Security/Badging Office, Security Manager, ASAP. The FSO will ensure that company employees selected to perform a Security function at NAVSOC will be JPAS, certified personnel and that such personnel have accounts and "read" access.

e. Basic Requirement. Personnel who are issued either an On-Site or Off-Site an identification badge and/or who are granted access to NAVSOC facilities and/or host installations must have, at a minimum, a current SECRET clearance under the sponsorship of the employing contractor. The contractor shall establish a system to immediately notify the NAVSOC Security Manager, and immediately deny access to NAVSOC facilities, when a contractor employee's clearance is withdrawn or administratively downgraded for any reason.

e. Security Classification Guide (SCG). The contractor shall ensure that the appropriate SCG is used to determine classification requirements for NAVSOC information and material. Questions regarding classification may be directed to the NAVSOC Security Manager.

II. Handling Classified Material or Information

a. Control and Safeguarding. Contractor personnel working at NAVSOC or traveling to support NAVSOC efforts are responsible for the control and safeguarding of all classified and sensitive material in their possession. All contractor personnel will be briefed by their company on their individual responsibilities to safeguard classified material. In addition, all contractor personnel authorized DoD Identification (i.e., Common Access Card (CAC)) are required to attend the Security Orientation Briefing prior to badge issuance (Contact respective NAVSOC Security Personnel for further information). In the event of possible or actual loss or compromise of classified material, the on-site Contractor point of contact (POC) at NAVSOC will immediately report the incident to NAVSOC Security Manager. This does not negate the need for the POC to promptly report the incident to the supported NAVSOC Technical Office management representative. A NAVSOC Security Manager Representative will conduct an inquiry of the incident and provide a report to the FSO and the Cognizant Field Office of the DSS if the event involves Contractor personnel. The contractor will promptly correct any deficient security conditions identified by the NAVSOC Security Manager.

b. Storage.

1. Collateral Secret classified material may only be stored in containers authorized by and registered in the NAVSOC Classified Document Library. Containers are assigned to a Primary Custodian and, where necessary, alternate custodians are appointed. On-site contractor personnel may act as custodians, but will be subject to inspection by NAVSOC government personnel at any and all times. Custodians must be properly listed on the Standard Form 700 and must be properly registered with and briefed on their custodial responsibilities. The contractor will assure that the Security Manager is promptly notified when their personnel no longer need access to a container and that all personnel to whom classified documents have been issued or that were custodians or are process out and have turn in all classified material to the Classified Material Custodian prior to their departure or relocating within NAVSOC. The custodian will notify the Security Manager when a container is to be relocated or turned in or when there is a change in personnel that are authorized access to the container. Custodians must also notify the Classified Material Custodian when collateral classified material requires a change of custody.

2. Only NAVSOC Security Manager approved areas are authorized for the open storage and processing of classified material. All other areas within NAVSOC facilities are governed by proper In-Use-Controls. The term "In-Use-Controls" is defined as: When classified material is removed from the container, appropriately cleared personnel with the requisite need-to-know must exercise physical control of the material at all times. Additionally, other controls such as closing the office blinds, positioning computer monitors, and/or shutting the office doors shall be utilized to preclude unauthorized disclosure of classified material/information.

c. Transmission of Classified Material.

1. All classified (collateral) material transmitted by mail or courier for use by Contractor or NAVSOC Staff will be addressed to:

Headquarters:	Detachment ALFA	Detachment CHARLIE	Detachment DELTA
Commanding Officer Naval Satellite Operations Center ATTN: N0021 661 13th St., Bldg.375 Point Mugu, CA 93042-5003	Officer-In-Charge Naval Satellite Operations Center Detachment ALFA Lighthouse Road Prospect Harbor, ME 04669-9999	Officer-In-Charge Naval Satellite Operations Center Detachment CHARLIE PSC 488 Box 112 FPO, AP 96537-1810	Officer in Charge Naval Satellite Operations Center Detachment DELTA 400 O'Malley Avenue, Suite 39 Schriever AFB, CO 80912-4039

The inner envelope will be addressed to the attention of the person for whom the material is intended.

2. All classified collateral material, (Confidential/Secret), that is hand carried to NAVSOC by contractor personnel must be delivered to the Classified Material Custodian (N0021) for processing.

3. All NAVSOC classified material that is transmitted from NAVSOC facilities, regardless of method (less faxing), will be processed by: the Classified Material Custodian. Contractors authorized to use secure faxes shall be appropriately trained as to their responsibilities prior to conducting such activity. All instances of secure facsimile operations and SIPRNET printer usage will be logged in accordance with current NAVSOC procedures.

4. NAVSOC classified material that is transmitted/carried within the NAVSOC protected perimeter of a NAVSOC facility or installation, shall be appropriately marked and have a classified cover sheet affixed. NAVSOC classified material that is transmitted/carried in a common area or between NAVSOC buildings (i.e., space accessible by uncleared personnel) shall be appropriately marked, have a classified cover sheet affixed, and placed in an opaque envelope.

III. Information Systems (IS) Security.

a. Contractors using NAVSOC information systems, networks or computer resources will comply with the provisions of applicable DoD and NAVSOC Directives and Instructions governing their use.

b. Contractor shall protect DoD sensitive unclassified data regardless of the location or ownership of the transport media, including, but not limited to mobile computing devices and removable storage media, whether Government furnished or contractor owned/leased. Contractor shall comply with all current information assurance and information security policies, procedures, and statutes applicable to DoD information technology, including the July 3, 2007 DoD CIO Policy Memorandum on Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media.

c. Access to NAVSOC information systems is limited to Government Staff and approved contractor employees who have been issued the requisite system privileges, as well as meeting security clearance and Need-To-Know requirements for access to classified systems. Under no circumstance shall a visiting or assigned contractor employee and/or representative obtain access

to, connect to, or otherwise interface with any NAVSOC information system (classified or unclassified) without prior written approval from the NAVSOC Information System Security Officer. This includes the attaching of unapproved laptops and other hardware peripherals to Local Area Networks and stand-alone systems.

d. The use of wireless computer technology (Bluetooth, 802.11X, RF, etc) within the NAVSOC enclave is prohibited without explicit written permission from the NAVSOC Designated Approval Authority (DAA). (This includes both contractor or NAVSOC provided radio-frequency wireless devices and networks.)

e. Contractors will use DoD information systems only for authorized purposes and never for personal business or prohibited uses. Prohibited uses include placing, downloading, or storing material onto computers or conducting Internet searches or otherwise accessing or using sites containing, or using government equipment and time to print, produce, or store material that society would consider to be pornographic, hate crime or gambling.

f. Contractors will not introduce or use unauthorized software, firmware, or hardware on any DoD information system, this includes the use of instant messaging software and peer-to-peer file sharing software.

g. Contractors will not unilaterally bypass, strain, or test information assurance mechanisms. If IA mechanisms must be bypassed, the contractor shall coordinate the procedure with the Information Assurance Office (IAO) and receive written approval from the Information Assurance Manager (IAM) or designated NAVSOC representative.

h. The loss, theft, destruction, or suspected compromise of any NAVSOC computer or computer systems will be immediately reported to the NAVSOC Security Manager. The contractor shall establish a system to assure that any NAVSOC issued or owned electronic equipment (e.g. telephone, computer, etc.,) is properly returned through proper NAVSOC channels prior to the departure of their personnel.

IV. Physical Security/Access Controls Procedures.

a. NAVSOC will provide appropriate response to emergencies occurring within NAVSOC facilities. The Contractor will comply with all emergency rules and procedures established.

b. All personnel assigned to or visiting NAVSOC facilities are subject to random inspections of their vehicles, personal items in their possession, and of their persons. Consent to these inspections is considered granted when personnel accept either a badge or a vehicle-parking pass that permits access into respective installations.

c. NAVSOC Security may, at their discretion, authorize the issuance of a DoD Common Access Card (CAC) identification badge for a period not to exceed the length of the basic contract or option period. The NAVSOC Security Manager and/or NAVSOC Contracting Officer's Representative (COR), in consonance with the local issuing office. A current copy of the DD-254 issued to either a Prime Contractor or Subcontractor, a current Visit Authorization Letter (VAL) and I9 Form must be on file prior to issuance. DoD CACs are the property of the U.S.

Government and will be worn and used for official business only. Identification badges must be worn above the waist in plain sight at all times within NAVSOC facilities. Lost or misplaced badges and access cards must be immediately reported to Security Manager (within one working day). Additionally, the FSO and the person to whom the CAC is issued shall promptly report a name change, clearance level change, or transfer. The contractor shall establish a system to assure that NAVSOC Administrative Division is promptly notified of such changes or when a person issued a NAVSOC badge is terminating employment with the company or is transferring within the company and will no longer require access to NAVSOC facilities. The need for transferring personnel to retain a CAC shall be determined by the Security Manager. The FSO shall be responsible for assuring that the badges for departing personnel are turned in to the corresponding issuing office prior to their departure.

1. NAVSOC Headquarters and Detachments having access card readers may consider requests by contractors for the issuance of an electronic facility access cards. Contractors will submit Badge Request Forms (as appropriate) and must have attended the Security Orientation Brief. The preparation and submission of the necessary forms for obtaining a badge is the responsibility of the contractor.

d. Contractor personnel not physically located/assigned to a NAVSOC installation, but who require routine access to facilities in the performance of their contract may be eligible for a temporary identification badge/pass (extended visitor badge).

e. All visits by contractor personnel require the submission of a VAL in accordance with the NISPOM. Visitors that are not issued CACs or extended visitor badges must notify the NAVSOC Security Office, respective Detachment Officer in Charge or designated On-Site security representative prior to each visit. VALs may be retained for one year, if requested. VALS shall be mailed, or faxed to:

Headquarters:	Detachment ALFA	Detachment CHARLIE	Detachment DELTA
Commanding Officer Naval Satellite Operations Center ATTN: Security Manager, N002 661 13th St., Bldg.375 Point Mugu, CA 93042-5003 Fax: 805-989-7140	Officer-In-Charge Naval Satellite Operations Center Detachment ALFA Lighthouse Road Prospect Harbor, ME 04669-9999 Fax: 207-963-7180	Officer-In-Charge Naval Satellite Operations Center Detachment CHARLIE PSC 488 Box 112 FPO, AP 96537-1810 Fax: 671-355-5405	Officer in Charge Naval Satellite Operations Center Detachment DELTA 400 O'Malley Avenue, Suite 39 Schriever AFB, CO 80912-4039 Fax: 719-567-3397

g. The contractor shall establish a system to ensure prior notification to the appropriate site representative, when visits to NAVSOC facilities by Foreign Nationals, to include those employed by the contractor, are desired. Request 30 days notice for foreign government representatives and 5 days notice for all other foreign visitors. The visit by a foreign national employee may require the possession of an Export Control License by the contractor and proof of such license may be required before the visit is approved. The contractor shall ensure compliance with all escort and badge requirements for foreign nationals.

V. Security Compliance Inspections.

NAVSOC Security personnel will conduct periodic inspections of NAVSOC facilities and off-site contractor facilities that are using NAVSOC computer systems. The contractor shall ensure that all contract personnel fully cooperate during these inspections. A report of the inspection

will be forwarded, through appropriate contract channels, to the contractor and the appropriate contractor's COR. The contractor will take prompt action to correct identified deficiencies.

VI. Reports.
As required by the NISPOM, contractors are required to report events that impact their facility clearance (FCL), an employee's personnel clearance (PCL), the ability to properly safeguard classified information, or an indication that classified information has been lost or compromised. The Contractor will ensure that when such events impact, or potentially impact NAVSOC personnel, operations, or information, they are also promptly reported to the Security Manager or Detachment Officer-In-Charge. Examples of such events include, but are not limited to the following:

a. The denial, suspension or revocation of a security clearance of any assigned person, or the suspension, revocation or denial of a FCL connected to a NAVSOC contract.

b. Any adverse information which would cast doubt on an assigned employee's continued suitability for continued access to classified information, material, or facilities;

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;

e. The loss, theft, or destruction of any NAVSOC issued or owned equipment or material.

VII. Escort Policy
The contractor shall comply with NAVSOC and detachment host installation escort policies.

VIII. Special Considerations for NAVSOC Enclave Facilities.
Any contractor occupied space within NAVSOC facilities will be used strictly for official business in support of NAVSOC efforts.

IX. Items Prohibited Within NAVSOC Facilities.
a. Dangerous weapons, instruments or devices. This 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 shots, blow guns, or any other device which uses gun powder, compressed gas or air, or spring tension to forcefully eject a projectile 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 knife with a blade longer than 2 ½ inches (Knives used for authorized construction and or repair efforts are excluded from this prohibition);
- Martial arts devices (throwing stars, nunchuks), stun guns, Tasers, brass knuckles, billy clubs, night sticks, pipe, bars, or mallets, or other similar devices capable of being used as a weapon;

- "Explosives" designed to, or having the capability to, cause death, serious bodily injury, or substantial material damage;
- "Other lethal devices" designed to or that have the capability to, cause death, serious bodily injury, or substantial damage to property through the release, dissemination, or impact of toxic chemicals, biological agents, or toxins or radiation or radioactive material;
- Any other item that may be used to inflict serious injury or death to another person or temporarily blind or disable an individual and which have not been specifically authorized by proper authority.

b. Explosive article or compound. This 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.

X. Contractor Check-Out Procedures

The contractor shall follow NAVSOC "check-out" procedures for all contract employees who have been issued CAC or visitor badges. The system shall ensure that all badges, keys, classified documents, equipment, communications security equipment (COMSEC)/material, etc., are turned in through proper NAVSOC channels prior to the employee's departure or transfer. NAVSOC Administrative Division shall issue a form that shall be used by contractor personnel to record the checkout process. Appropriate NAVSOC personnel shall verify the checkout form.

XI. Investigations and Inquiries

NAVSOC Security personnel may be required to conduct various investigations or inquiries in which contractor employees may be involved. The contractor shall ensure that all contract personnel fully cooperate with NAVSOC Security representatives during these efforts. Information and documents requested by NAVSOC representatives will be promptly provided in compliance with Federal and State law and regulation. A report of the inquiry or investigation will be forwarded, through appropriate contract channels, to the Contractor's employing facility and COR. The contractor will take prompt action to correct identified deficiencies and will provide a written report of the actions taken through contract channels to the Security Manager or detachment Officer-In-Charge.

XII. Clearance for Public Release

All appropriate information resulting or derived from NAVSOC funded efforts that are intended for public release must be submitted for NAVSOC approval in accordance with applicable directives.

XIII. Preparation of DD Forms 254

a. Subcontracts. The contractor shall ensure that NAVSOC security requirements, to include the appropriate SCG, are passed down to their subcontractors who are involved in NAVSOC efforts. A copy of all DD Forms 254 issued to subcontractors performing NAVSOC work will be provided to the NAVSOC COR. Contractors will ensure that all DD Forms 254 are kept current.

b. Employee Knowledge of Security Requirements. The contractor shall assure that all of their employees who are assigned to support NAVSOC are thoroughly familiar with DoD security regulations and requirements.

XIV. Foreign Travel

Contractors who have been badged and who are traveling to foreign countries shall complete a foreign travel briefing. The contractor shall also review mandatory briefings. This requirement does not relieve the contractor of security reporting requirements mandated by his or her organization.

XV. NAVSOC Security Manager Website Tools

NAVOSC maintains an internal (NAVSOC Intranet "SATWEB") and external (Internet) website. Forms referenced in this document, as well as other pertinent information, are provided on these and host installation websites.

XVI. Contractor Security Education and Training Program

The contractor shall ensure that all personnel assigned to support NAVSOC, and that are issued badges, are made aware of these and other NAVSOC security requirements.