DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)

OMB No. 0704-0567
OMB approval expires: August 31, 2028

The public reporting burden for this collection of information, 0704-0567, is estimated to average 36 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See Instructions)*

Secret

b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY

None (See instructions)

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

☐ **a. PRIME CONTRACT NUMBER** *(See instructions.)*

☐ **b. SUBCONTRACT NUMBER**

☒ **c. SOLICITATION OR OTHER NUMBER** N3220526R6057 **DUE DATE** *(YYYYMMDD)*

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

☒ **a. ORIGINAL** *(Complete date in all cases.)* **DATE** *(YYYYMMDD)*

☐ **b. REVISED** *(Supersedes all previous specifications.)* **REVISION NO.** **DATE** *(YYYYMMDD)*

☐ **c. FINAL** *(Complete Item 5 in all cases.)* **DATE** *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☒ No ☐ Yes *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? ☒ No ☐ Yes *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(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*

7. SUBCONTRACTOR(S) *(Click button if you choose to add or list the subcontractors -- but will still require a separate DD Form 254 issued by a prime contractor to each subcontractor)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*

8. ACTUAL PERFORMANCE *(Click button to add more locations.)*

a. LOCATION(S) *(For actual performance, see instructions.)*	b. CAGE CODE *(If applicable, see Instructions.)*	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
Commander, Submarine Force U.S. Pacific Fleet 1430 Morton St. Bldg. 619 Pearl Harbor, HI 96860-4664 Building 1310		Commander, Submarine Force U.S. Pacific Fleet 1430 Morton St. Bldg. 619 Pearl Harbor, HI 96860-4664 Building 1310

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

Vessel to provide logistics support and services to Commander, Submarine Forces, U.S. Pacific Fleet in support of offshore personnel and supply transfers.

10. CONTRACTOR WILL REQUIRE ACCESS TO: *(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- ☐ **a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION**
- ☐ **b. RESTRICTED DATA**
- ☐ **c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)** *(If CNWDI applies, RESTRICTED DATA must also be marked.)*
- ☐ **d. FORMERLY RESTRICTED DATA**
- **e. NATIONAL INTELLIGENCE INFORMATION:**
  - ☐ **(1) Sensitive Compartmented Information (SCI)**
  - ☐ **(2) Non-SCI**
- ☐ **f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION**
- ☐ **g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION**
- ☐ **h. FOREIGN GOVERNMENT INFORMATION**
- ☐ **i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION**
- ☒ **j. CONTROLLED UNCLASSIFIED INFORMATION (CUI)** *(See instructions.)*
- ☐ **k. OTHER** *(Specify)* *(See instructions.)*

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: *(X all that apply. See instructions. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- ☒ **a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY** *(Applicable only if there is no access or storage required at contractor facility. See instructions.)*
- ☐ **b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY**
- ☐ **c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL**
- ☐ **d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE**
- ☐ **e. PERFORM SERVICES ONLY**
- ☐ **f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S.,PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES**
- ☐ **g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER**
- ☐ **h. REQUIRE A COMSEC ACCOUNT**
- ☐ **i. HAVE A TEMPEST REQUIREMENT**
- ☒ **j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS**
- ☐ **k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE**
- ☒ **l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI).** *(DoD Components: refer to DoDI 5200.48, only for specific CUI protection requirements. Non-DoD Components: see instructions.)*
- ☐ **m. OTHER** *(Specify)* *(See instructions.)*

12. PUBLIC RELEASE

Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual (NISPOM) or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified here with at least office and phone contact information and if available, an e-mail address. *(See instructions)*

☒ **DIRECT** ☐ **THROUGH** *(Specify below)*

Public Release Authority:
Military Sealift Command, Public Affairs Office, Code N00P
471 East C Street Bldg SP-48. Norfolk, VA 23511-2419

13. SECURITY GUIDANCE

The security classification guidance for classified information needed for this 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. The field will expand as text is added. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. Also allows for up to 6 internal reviewers to digitally sign. See instructions for additional guidance or use of the fillable PDF.)

Item 1(a)/1(b): This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret." The Contractor shall comply with-The Security Agreement DD Form 441), including the Part 117 of Title 32 CFR; and any revisions to that manual, notice of which has been furnished to the Contractor. If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract. The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

Item 8(a): Actual performance location of classified work, and contractor access to classified is restricted to actual performance locations defined in Item 8(a) of this form.

Item: 10(j): All Controlled Unclassified Information (CUI) associated with this contract must be protected per the guidance provided for Item 11(l) of this DD Form 254.

Item 11(a): Contractor shall have access to SECRET classified information regarding mission operations. Employment must be by U.S. citizens and possess at least a SECRET clearance. All designated personnel who maintain a security clearance and handle classified information must attend Counterintelligence Awareness and Reporting (CIAR) training. See DoDD 5240.06, Counterintelligence Awareness and Reporting, for guidance. The Contractor shall ensure that any classified information disclosed to its employees is no further released or made available to other employees, or any other person who does not have a comparable clearance and a "Need to know". The COR will provide the contractor with applicable Derivative Classification guidance in addition to requirements in DoDM 5200.01-V3.

Item 11(a) continued: Personnel Clearance (PCL). All personnel performing on or supporting this contract in any way shall be U.S. citizens. The personnel security requirements for this contract require contractor personnel to possess the interim or final Secret security clearance eligibility when performance starts. All personnel requiring Secret eligibility under this contract shall undergo a favorably adjudicated Tier 3 (T3) investigation or equivalent investigation as applicable. Enrollment into Continuous Evaluation, and PVQ date must be current within 5 years, and reflected in DISS, along with proper SMO ownership/servicing throughout the contract.

Item 11(a) continued: All contractors with access to classified information systems are required to receive the NATO awareness briefing, and responsibilities for safeguarding NATO classified information, and acknowledge receipt of the brief in writing. Actual knowledge of, generation, or production of NATO information is not required for performance on the contract. The Government Sponsor/Mission Sponsor (COR, PM, PO) shall be responsible for limiting access to Secret classified information to the absolute minimum amount of contractor personnel required in performance of the contract. The Government Sponsor, and contractor personnel shall ensure that any classified information disclosed to them, is no further released or made available to other personnel, who do not have a comparable clearance and need-to-know.

Item 11(j): The Contractor shall utilize the Military Sealift Commands' Critical Information and Indicators List, which will be identified or provided by the Contracting Officer or Contracting Officer Representative to help identify and protect critical information associated with this contract. During the performance period of this contract, the Contractor may be exposed to, use, or produce, MSC Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. MSC's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI). MSC's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites. Media requests related to this project shall be directed to MSC Public Release Authority listed in Item 12 of this DD Form 254. Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive and Company Proprietary information related to this contract or other programs must be immediately reported to the Facility Security Officer, DCSA and/ or the Naval Criminal Investigative Service. Performance under this contract requires the contractor to adhere to OPSEC requirements IAW DODM 5205.02, OPSEC Program Manual. OPSEC requirements are additional to the requirements of Part 117 of Title 32 CFR, therefore, the Contractor may not impose OPSEC requirements on its subcontractors unless MSC approves the OPSEC requirements.

Item 11(l): All Controlled Unclassified Information associated with this contract must be safeguarded to prevent unauthorized public disclosure. CUI such as FOUO, SCG, and other technical information are not authorized for public release and cannot be placed on a publicly accessible web site or web server. All emails containing such information or attachments, shall be protected per NIST SP-800-171, or subsequent revisions. All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast, etc.) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.) are prohibited. Destroy all CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction.

Item 11(l) continued: The Contractor shall implement InfoSec measures for its contractor furnished unclassified information technology system(s) used in performance of this contract. InfoSec measures shall be compliant with DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. At a minimum, the security standards extracted from the referenced National Institute of Standards and Technology (NIST) Special Publication 800-171, Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations or accepted equivalents, shall be incorporated into any InfoSec program the contractor establishes.

List of Attachments (All Files Must be attached Prior to Signing, i.e., for any digital signature on the form)

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
LTJG Jonathan Bagley Contracting Officer Rep (COR)	BAGLEY.JONATHAN.MICHAEL.1412276066 Digitally signed by BAGLEY.JONATHAN.MICHAEL.1412276066 Date: 2026.06.24 09:27:35 -10'00'
NAME & TITLE OF REVIEWING OFFICIAL	**SIGNATURE**
Tim Vickers MSC PM41 Project Officer	VICKERS.TIMOTHY.CHARLES.1095482844 Digitally signed by VICKERS.TIMOTHY.CHARLES.1095482844 Date: 2026.06.25 15:44:04 -04'00'

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
LT Zalai ParedesSojo SRS-33 Security Officer	PAREDESSOJO.ZALAI.C.1300392802 Digitally signed by PAREDESSOJO.ZALAI.C.1300392802 Date: 2026.06.29 11:41:37 -10'00'
NAME & TITLE OF REVIEWING OFFICIAL	**SIGNATURE**
MSC OPSEC Officer	REILLY.PHILIP.FRANCIS.1364161464 Digitally signed by REILLY.PHILIP.FRANCIS.1364161464 Date: 2026.07.01 09:19:12 -04'00'
NAME & TITLE OF REVIEWING OFFICIAL	**SIGNATURE**
Damien Holmes MSC Industrial Security Program Manager	HOLMES.DAMIEN.LAMONT.1142398229 Digitally signed by HOLMES.DAMIEN.LAMONT.1142398229 Date: 2026.07.01 09:46:40 -04'00'

14. ADDITIONAL SECURITY REQUIREMENTS

Requirements, in addition to NISPOM requirements for classified information, are established for this contract.

☐ No ☒ Yes *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 CSO. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

1. All members who require access to classified information, sensitive information, controlled unclassified information (to include Privacy Act and Personally Identifiable Information (PII)) or access to the classified information network shall comply with DoDM 5200.01 Vol I - III (DoD Information Security Program), SECNAVINST 5510.36 (SECNAV Information Security Program), DoDD 5240.06 (Counterintelligence Awareness and Reporting - CIAR), and 32 CFR, Part 117 (NISPOM).
2. Contractor must provide VISIT AUTHORIZATION REQUEST (VAR), via DISS, listing all contract personnel located on installations and on-board ships that require or will have access to classified information as well as other contractors that perform contractual services on Government installations/facilities or on-board ships and require or have access to sensitive unclassified information or those that require routine or frequent "entry" to the installation or on board ships in the performance of other types of contracts, services or maintenance. During the performance period of the contract, the Facility Security Officer, shall notify Command Security Manager within 24 hours of any changes to the listing of the contract personnel.
3. Contractor personnel shall comply with all local security requirements including entry and exit control for personnel and property at the government facilities. Contractor employees shall be required to comply with all Government security regulations and requirements. Initial and periodic safety and security training and briefings will be provided by Government personnel. Failure to comply with Government security regulations and requirements shall require the company to provide the Government with a written remediation/corrective action plan; furthermore, failure to comply with such requirements can be cause for removal and the contractor will not be able to provide service on this contract.
4. Briefings: The Contractor shall ensure all new employees are provided a reporting briefing covering security indoctrination for access to classified and/or sensitive information, building access control procedures, key control, government property control, and the introduction of prohibited items in restricted spaces, action to be taken in the event of emergency situations (bomb threat, fire), Anti-Terrorism/Force Protection, and information systems security awareness. Contractor shall further ensure annual security training is provided to all employees, and includes but is not limited to; Annual Security Stand-down, Derivative Classification, Counterintelligence Awareness Training, Anti-terrorism Level I, Cybersecurity Awareness, OPSEC, and Active Shooter. This may be conducted on-line through computer based training or through All Hands podium sessions. Counterintelligence training must be received through NCIS; on-line training is authorized only in the event NCIS is not available to provided required training. Records of training shall be maintained for duration of the contract. Records shall contain employee name, type, and date of training. Contractors are required to complete training listed in the MSC Annual Mandatory Training list, which shall be provided by the COR.
5. Badges/Common Access Card (CAC): In accordance with Homeland Security Presidential Directive (HSPD)-12; Policy for a Common Identification Standard for Federal Employees and Contractors, and it's implementing directives; Contractor and Contractor employees requiring physical access to any area of a federally controlled base, facility or activity, and/or requiring access to a DoD computer/network under this contract shall meet HSPD-12 and FIPS credentialing standards for issuance of the Common Access Card (CAC)/Facility Badge. The Contractor shall comply with the host installation and MSC regulations for obtaining personnel identification, facility, and vehicle passes (if required). The Contractor shall ensure that every on-site employee applies for and receives a Base Access Control Badge/CAC prior to the start of full contract performance. The Contractor shall ensure that all employees display their Personal Identity Verification (PIV) card (e.g. CAC/Facility Badge) above the waist, ensuring that they are visible at all times while on to the base and assigned facilities. The Contractor shall also ensure that all credentials (i.e. facility/base passes, CACs, etc.) are returned to the COR/ACOR and/or the government Cognizant Security as employees are dismissed or terminated, and when the contract expires. All Contractor personnel are required to conform to all operational site and base regulations, to include but not limited to: designated routes, parking regulations, base vehicle speed limits, automotive liability insurance, excavation permits, use of cellular, mobile, radio phones, photographing base facilities, infrastructure, restricted areas prohibited items.
6. Information Security. Contractor employees shall follow applicable DoD/DoN instructions, regulations, policies and procedures when reviewing, processing, producing, protecting, destroying and/or storing sensitive and/or classified information. Contractor shall have a Need to-Know for access to sensitive and/or classified spaces in performance of contract duties. The Contractor shall take appropriate precautions to prevent security violations, ensure all compromises, suspected compromises, attempted penetration and/or loss of sensitive and/or classified material is reported in person or by phone call within 15 minutes of discovery to the COR/ACOR and the government cognizant

Security Manager. Contractor will provide all assistance required for completion of the security Preliminary Inquiry directed by COMSC, COR, and/or Command Security Manager. The Contractor shall take appropriate precautions to prevent security violations, and promote a high level of security awareness among personnel assigned to this contract.

7. Privacy Act: Information required or generated under this contract may be subject to the Privacy Act. Work on this project requires that Contractor personnel have access to Privacy Information. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations. Contractor personnel may be required to sign a Non-Disclosure Form.

8. Internet Access and Email: The Contractor is authorized to use the Government's email systems with approved background investigation. Contractor shall abide by all DOD and DON regulations for proper use of Information Systems. Contractor personnel must take personal responsibility for Operations Security (OPSEC) using all Government Information Systems. Military and Government information/data/ pictures shall not be forwarded to non-military internet service providers or placed on public web sites. The Contractor shall participate in OPSEC/Internet Threat Awareness training.

9. Non-Disclosure of Data: The Contractor and its personnel and subcontractors shall only disclose data obtained, received, or learned as a result of performance of this contract to Contractor personnel directly performing under this contract and to United States Department of Defense personnel to whom disclosure of such data is required in performance of this contract. The Contractor, its personnel and subcontractors, shall not disclose such data to anyone who prepares offers, proposals, bids, and/or quotations for Government and/or non-Government procurements. The Contractor and its personnel and subcontractors shall take all steps necessary to prevent disclosure of such data except as specifically permitted herein.

15. INSPECTIONS

Elements of this contract are outside the inspection responsibility of the CSO.

☐ No ☒ Yes *If Yes, explain and identify specific areas and government activity responsible for inspections. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

Ship inspections will be conducted by Submarine Readiness Squadron (SRS) 33.

16. GOVERNMENT CONTRACTING ACTIVITY (GCA) AND POINT OF CONTACT (POC)

a. GCA NAME	c. ADDRESS *(Include ZIP Code)*	d. POC NAME
Commander, Military Sealift Command	Commander, Military Sealift Command 471 E. C St. Bldg. SP-64 Norfolk, VA 23511	LT(jg) Jonathan Bagley
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*		**e. POC TELEPHONE** *(Include Area Code)* +1 (808) 473-1474
N32205		**f. EMAIL ADDRESS** *(See Instructions)* jonathan.m.bagley2.mil@us.navy.mil

17. CERTIFICATION AND SIGNATURES

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. Upon digitally signing Item 17h, no changes can be made as the form will be locked.

a. TYPED NAME OF CERTIFYING OFFICIAL *(Last, First, Middle Initial) (See Instructions)*	d. AAC OF THE CONTRACTING OFFICE *(See Instructions)*	h. SIGNATURE
Davis, Danny	N32205	DAVIS.DANNY.WAYNE.JR.1115338311 Digitally signed by DAVIS.DANNY.WAYNE.JR.1115338311 Date: 2026.07.01 14:07:36 -04'00'
b. TITLE	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)*	
Contracting Officer		
c. ADDRESS *(Include ZIP Code)*	**f. TELEPHONE** *(Include Area Code)*	**i. DATE SIGNED** *(See Instructions)*
Military Sealift Command 471 E. C St. Bldg. SP-64 Norfolk, VA 23511	+1 (564) 226-8891	01-JUL-2026
	g. EMAIL ADDRESS *(See Instructions)* danny.w.davis1.civ@us.navy.mil	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

- ☒ **a. CONTRACTOR**
- ☐ **b. SUBCONTRACTOR**
- ☒ **c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR**
- ☐ **d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION**
- ☒ **e. ADMINISTRATIVE CONTRACTING OFFICER**
- ☒ **f. OTHER AS NECESSARY** *(If more room is needed, continue in Item 13 or on additional page if necessary.)*

MSC Security