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 70 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)*

TOP SECRET

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

SECRET

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

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

☐ **b. SUBCONTRACT NUMBER**

■ **c. SOLICITATION OR OTHER NUMBER** N6600126R3608 **DUE DATE***(YYYYMMDD)* 20260526

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

■ **a. ORIGINAL** *(Complete date in all cases.)* **DATE***(YYYYMMDD)* 20260526

☐ **b. REVISED** *(Supersedes all previous specifications.)* **REVISON 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 marterial 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 contractors request dated , retention of the classified material is authorized for the period of: days

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)*
TBD	TBD	

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)*
TBD United States	TBD	
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)*
Naval Information Warfare Center (NIWC) Pacific 53560 Hull Street San Diego, CA 92152-5001 United States		

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

The main objective of this effort is to modernize and align Naval Command and Control for Integrated Joint/Coalition Fires and make it deployable to afloat and ashore sites such as the Carrier Strike Groups (CSG) to include CRUDES/DDGs and Carrier Airwing assets, Expeditionary Strike Group (ESG), Marine Corps NMESIS, Army HIMARS, Airforce assets, Coalition Forces, Tactical Fleet Command Centers (TFCC), Operational Command Post (OCP) and the Maritime Operations Centers (MOC). This effort will enhance the warfighters decision-making and information gathering effectiveness by integrating and taking advantage of Machine Learning/ Artificial Intelligence (ML/AI) approaches. The intent is to mature / modernize the technologies, increase their Technology Readiness Level (TRL) and prepare them for transition to a number of possible Programs of Record (PoR). This effort will include providing prototype validation, research and development, software development, implementation, test and verification for advanced C2 techno1ogies. Specifically, this effort will provide development of software products utilizing microservices, containers, service mesh, and kubernetes previously explored under the C2X project for use in command and control environment. The development work will include the design and implementation of container-based software, research and performance characterization of C2 application functionality, Artificial Intelligence, Machine Learning, Operations Research (AI/ML/OR), capturing and validating user stories, workflows, applying cybersecurity best practices, utilizing a DEVSECOPS pipeline, and related Navy Mission Essential Tasks, and development of associated technical documentation.

Solicitation Number: Old N6600126R0034 ECD: To be added at time of award.

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

- [x] **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:**
  - [x] **(1) Sensitive Compartmented Information (SCI)**
  - [x] **(2) Non-SCI**
- [ ] **f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION**
- [x] **g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION**
- [ ] **h. FOREIGN GOVERMENT INFORMATION**
- [ ] **i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION**
- [x] **j. CONTROLLED UNCLASSIFIED INFORMATION (CUI)** *(See instructions.)*
- [x] **k. OTHER** *(Specify)* *(See instructions.)*
  See Block 13 - Ref 10K

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: *(X all that apply. Provide details in Block 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**
- [x] **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**
- [x] **h. REQUIRE A COMSEC ACCOUNT**
- [ ] **i. HAVE A TEMPEST REQUIREMENT**
- [x] **j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS**
- [ ] **k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE**
- [x] **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.)*
- [x] **m. OTHER** *(Specify)* *(See instructions.)*
  See Block 13 - Ref 11M

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**
- [x] **THROUGH** *(Specify below)*

Naval Information Warfare Center (NIWC) Pacific, Code 85000, 53560 Hull Street, San Diego, CA 92152-5001

Public Release Authority:
All information belonging to or provided by NIWC Pacific under this contract shall receive approval prior to release of information.

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.)

The DD 254 will be housed within the NCCS through the life of the contract. The Contractor shall be registered within NCCS at time of award to gain access to the DD 254. It is incumbent upon the Contractor to ensure that the necessary security paperwork is submitted in sufficient time to enable each individual to be cleared prior to beginning work on this contract. In the event that the NCCS is superseded by another System of Record, the same requirements apply.

Block 12 Continuation: Release of SCI, Non-SCI and NATO (Read-on IA W with the National Intelligence Security Policy Directive 17-008; NATO access is not required on this contract, see phrase 1 0.g/k(l)) material is not au horized.
Security Classification Guide (SCG): SCG to be provided under separate cover by the COR. MTC2 SCG.

The Project Manager (PM) Clemente Rivetti, Code 53223, (619) 299-4400, email: clemente.d.rivetti.civ@us.navy.mil.

Contracting Officer's Representative (COR) Howard L. Dyckman, Code 71730, (619) 553-3829, email: howard.l.dyckman.civ@us.navy.mil.

Direct all questions to the SCI Contracting Officer's Representative (COR) Clemente Rivetti, Code 53223, (619) 299-4400, email: clemente.d.rivetti.civ@us.navy.mil or the SCI Alternate COR (ACOR) Christina Nuibe, Code 53208, (619) 553-4533, email: christina.nuibe.civ@us.navy.mil.

The Contract Specialist (CS) Magda Velarde, Code 22530, (619) 947-1934, email: magda.v.velarde.civ@us.navy.mil.

-Prime contractors are required to send copies of all subcontract DD Form 254s to obtain flow-down approvals as required to the distribution listed in block 18: NIWC Pacific Code 53223/53208 (SCI CORs), 22530 (CS) see above and 83310 - Security - NIWC _PAC_ SecurityCOR@us.navy.mil.

The NIWC Pacific-COR will specify which positions require a clearance.

IT Level The COR shall determine the appropriate IT Level for each individual Contractor personnel in accordance with DoD Manual, DOD 8570.01M, Cyberspace Workforce Qualification and Management Program ; contractors will be transitioning to requires listed in DoD M 8140.01, "Cyberspace Workforce Management" in the near future.

Privileged Access Agreements (PAA) for CSWF/Sysadmin personnel

(A) SECNAVINST 5510.30C, Department of the Navy Personnel Security Program, 24 Jan 2020
(B) SECNAVINST 5239.20A, DoN Cyberspace IT and CSWF Management and Qualifications, 10 Feb 2016
(C) SECNAV Manual M-5239.2, Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual, June 2016

Reference (A) requires that a favorable Tier 5 (T5) background investigation or T5 reinvestigation (T5R every 5 years) be conducted on military, civilian and contractor personnel for privileged access IT. Reference (B) outlines the requirements for personnel needing privileged access. Reference (C) defines enhanced user requirements.

**Contractor personnel requiring administrative level access to network devices are required to possess a Secret clearance with a completed T5/T5R investigation to comply with cybersecurity policy.

Contractors shall follow all Host Command security and training requirements.

Personnel designated as derivative classifiers shall receive derivative classification training prior to access from the contractor's Facility Security Officer (FSO). The FSO shall ensure personnel receive initial and annual training during the life of this contract. Evidence of completion, training certificates or equivalent, shall be provided to the COR/TPOC no later than the individual's due date.

-Destruction of classified documents shall be by using National Security Agency (NSA) approved destruction equipment listed on the NSA/CSS evaluated products list (EPL) or other approved method for destroying classified information.

-All security related issues, incidents, or requests pertaining to this contract shall be presented in writing by the contractor's Facility Security Officer (FSO) to the individual identified in blocks 16, 17 and the COR of this DD254. The contractor shall abide by other reporting requirements outlined in the 32 CFR NISPOM Rule 117.8.

Per DoDD 5138.13 Para 4.1.e. and SECNAVINST 3820.3F, the Intelligence Oversight verbiage needs be included in all SOWs/254s. See below

INTELLIGENCE OVERSIGHT

For any contractor personnel conducting Intelligence or Intelligence-related activities or supporting those efforts under Department of Defense authorities shall report any Questionable Intelligence Activity (QIA), Significant, or Highly Sensitive Matter (S/HSM) to the Naval Information Warfare Systems Command Intelligence Oversight Program Manager or Senior Intelligence Officer.

Questionable Intelligence Activity (QIA): Any Intelligence or Intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

Significant or Highly Sensitive Matter (S/HSM): An Intelligence or Intelligence-related activity (regardless of whether the Intelligence or Intelligence-related activity is unlawful or contrary to an Executive Order, Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by Intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of Intelligence activities. Such matters might involve actual or potential:

Congressional inquiries or investigations
Adverse media coverage
Impact on foreign relations or foreign partners
Systemic compromise, loss, or unauthorized disclosure of protected information.

Changes: Solicitation DD254 resubmitted under a New Number: N6600126R3608. The solicitation number needed to be changed because the number was accidentally used for another procurement. Originally was submitted under Solicitation Number N6600126R0034 and Validated by Code 874 20260506.

Access Requirements:

10.a Further disclosure, to include subcontracting, of COMSEC information by a contractor requires prior approval of the NIWC Pacific COR. Access to any COMSEC information requires special briefings at the contractor facility. Access to classified COMSEC information requires a final U.S. Government clearance at the appropriate level. Use of COMSEC information is governed by the NSA Industrial COMSEC Manual, NSA/CSS Policy Manual 3-16 and 32 CFR Part 117 NISPOM Rule - 117.21. Contractors that will be designated CMS users must attend an initial CMS user training class that is given by the NIWC Pacific CMS office. If you have questions call (619) 553-5065. (Access is for COMSEC equipment/material).

10.e(1) The NAVWAR SIO has exclusive security responsibility for all SCI classified material released or developed under this contract. Defense Counterintelligence Security Agency (DCSA) is relieved of security inspection responsibility for all such material but retains responsibility for all non-SCI classified material released to or developed under this contract. Further disclosure to include subcontracting of SCI is prohibited until approval is received from the SCI cleared NIWC Pacific COR, NIWC Pacific Code 874 and NAVWAR SIO. Access to SCI information requires a final U.S. Government clearance at the appropriate level and will be performed within U.S. Government facilities only. Approval for SCI access, to enter spaces, attend meetings, and briefings in accordance with the PWS/SOO/SOW. No SCI deliverables can be produced.

The NIWC PAC SSO will recognize the noted estimated completion date (ECD) in block 9 upon contract award as the completion date for the contract. The SSO will initiate action to debrief contractor personnel with access to this contract unless extensions or modifications to the contract are received by the SSO office no later than 30 days after the established completion date.

Contractor personnel assigned to this effort who require access to SCI data and spaces must possess a current SSBI/T5/T5R with ICD 704 eligibility (which replaced DCID 6/4 eligibility) and be enrolled in Continuous Vetting.

Access to sub compartments may be required in order to comply with NISPD 002-22. SSO will provide sub compartment access as required on an individual basis.

Contract performance for SCI access is restricted to NIWC Pacific, San Diego, CA.

10.e(2) Prior approval from the NIWC Pacific COR and NIWC Pacific Code 874 is required for sub-contracting.

10.g/k(l) Effective immediately all contractor personnel with SCI access must be read-on NATO secret with an entry into Defense Information System for Security(DISS) prior to being granted access. This contract requires SCI cleared personnel to access JWICS/SIPRnet. In addition the contractor shall complete the derivative classification training; the special NATO briefing and derivative classification briefing are provided by the contracting company's facility security officer. This requirement is mandated per the national intelligence security policy directive 17-008. This read-on meets the mandated requirement; however, contractor does not require access to NATO on this contract. Contractor is not authorized to have NATO at its contractor's facility. JWICS/SIPRnet under the NA VW AR Claimancy is not accredited and/or authorized to receive or process NATO restricted up to NATO secret data. The contractor shall not use JWICS/SIPRNET for anything except that which is required for this contract. Questions, contact the GCA NATO Control Office 619-553-3005/3191. Subcontract DD254s require approval from the GCA NCO prior to access being granted. Policies: DOD M-5200.1 Volume 1, enclosure (3), SECNAVINST 5510.36B and USSAN 1-07.

10.j Contractors receiving, transmitting or accessing controlled unclassified information (CUI) on or through its contractor information system(s) must safeguard the information to avoid compromise, including but not limited to disclosure of information to unauthorized persons, unauthorized modification, destruction, or loss of an object, or the copying of information to unauthorized media, as required per DFARS subpart 204.73 and clauses 204-7304 and 252.204.7012, as well as NIST SP 800-171 series, which identifies the baseline CUI system security requirements for industry.

DoD contracts must also require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

Contractors shall report to the DOD each cyber incident that affects unclassified controlled technical information residing within or transiting contractor information systems in accordance with DFARS clause 204.7304 and 252.204-7012. Detailed reporting criteria and requirements are set forth in the clause at 252.204-7012, safeguarding of unclassified controlled technical information. For information on handling CUI see DODI 5200.48.

Controlled Unclassified Information (CUI) associated with this contract must be safeguarded to prevent unauthorized public disclosure. CUI such as Security Classification Guides (SCG), and other technical information with Distribution Statements B, C, D, E or F 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 must be appropriately marked and digitally signed and encrypted if being transmitted. All transmissions to personal email accounts (AOL, GMAIL, 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.
CUI Courses and Resources Created for Industry:
The Center for Development of Security Excellence (CDSE) has developed an eLearning course titled "DoD Controlled Unclassified Information (CUI) Training For Contractors (IF141.06.FY21.CTR) or the training can be taken on TWMS.
Additionally, CDSE has a CUI Toolkit available at https://www.cdse.edu/toolkits/cui/current.html. The Toolkit includes training, policy documents, resources, and an FAQ video.
Review the DoD CUI Registry at https://www.dodcui.mil to become familiar with CUI organizational index groupings and CUI categories.
Policy documents addressing CUI oversight: Do DI 5200.48 "Controlled Unclassified Information. "(https ://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF)
32 CFR 2002 Part IV National Archives and Records Administration 32 CFR Part 2002 "Controlled Unclassified Information" (https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf)
E.O. 13556 Vol 75, No 216. "Controlled Unclassified Information" (https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-283 60. pdf)
NIST Special Publication 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (https://csrc.nist.gov/pubs/sp/800/171/r3/final).

10.k(2) Some contractor personnel that work on Top Secret and below requirements and do not fall under phrase 10.g/k(1) are only required to receive the NATO Awareness Brief for the sole purpose of accessing SIPRnet. The special briefing is provided by the contracting company's Facility Security Officer (FSO). Note: do not add this awareness brief to in DISS. The contractor shall complete Derivative Classification training prior to being granted access to SIPRnet; training is provided by the company s FSO. Evidence of completion, training certificates or equivalent, shall be provided to the NATO Control Officer when requested. The contractor shall not use the SIPRNET for anything except that which is required for this contract. SIPRnet under the NAVWAR Claimancy is not accredited to receive or process NATO restricted up to NATO secret data. Questions, contact the GCA NATO Control Office 619-553-3005/3191. Policies: DOD M-5200.01 Volume 1, enclosure (3) and SECNAVINST 5510.36B.

11.c Any classified information generated in performance of this contract shall be marked according to Executive Order 13526 dtd 29 December 2009. Any extracts must apply derivative classifications and markings consistent with the source documents. Use of "Multiple Sources" on the "Derived From" line necessitates compliance with the 32 CFR Part 117 NISPOM Rule. Your Defense Counterintelligence Security Agency (DCSA) Industrial Security Representative (IS Rep) should be contacted for assistance. Classified material generated in support of this contract shall be classified in per its source material or SCG. Automated Information Systems (AIS) must be certified and accredited by the Cognizant Security Agency (CSA) prior to processing classified information associated with this contract.

11.h A COMSE account must be established when accountable COMSEC material is to be provided, acquired, or produced under a contract. A COM SEC account required: 17he contractor shall comply with the provisions of the NSA CSSM 3-16 and 32 CFR Part 117 NISPOM Rule. The NSA COR has primary responsibility for the auditing of all COMSEC material governed by the NSA CSSM 3-16. The Cognizant Security Office is responsible for inspecting for compliance with the COMSEC Supplement to the NISPOM. Contractor is required to have a COMSEC account at its contractor's facility. Contractor required to test and provide classified modeling and simulation to the C2X ODIE Lab via SDREN.

11.j Contractors are required to take Operation Security training. SECNAVINST 3070.2A, Operations Security, released May 9th, 2019, directs that all personnel requesting access to any DON networks (an account on NMCI, RDTE, etc.) must receive formal OPSEC training prior to approval for access to any DON networks, and at least annually thereafter. This requirement applies to all Government Civilian, Military and Contractor personnel who require access to DON networks. For contractors, this requirement applies whether or not OPSEC is currently listed as specific contract requirement.

Contractor Personnel with access to NMCI or Local RDT&E network and are registered in TWMS: Requirement is met when you complete yearly OPSEC COI in TWMS. This training must be completely yearly.
- Total Workforce Management Services (TWMS): https://twms.dc3n.navy.mil/selfservice/login.asp; must have a CAC to access this site.

Contractor Personnel access to NMCI or Local RDT&E network who are NOT registered in TWMS: Complete the training at one of the below sites and submit your certificate of completion to the RDT&E Operations Center (ROC). This training must be completely yearly.
- CDSE OPSEC Course: https://securityawareness.dcsa.mil/opsec/index.htm

The RDT&E Operations Center will verify OPSEC training is within the last year and a certificate is attached to the Hub request form.

Also see OPSEC attached for additional information.

11.l Contractors receiving, transmitting or accessing controlled unclassified information (CUI) on or through its contractor information system(s) must safeguard the information to avoid compromise, including but not limited to disclosure of information to unauthorized persons, unauthorized modification, destruction, or loss of an object, or the copying of information to unauthorized media, as required per DFARS subpart 204.73 and clauses 204-7304 and 252.204.7012, as well as NIST SP 800-171 series, which identifies the baseline CUI system security requirements for industry.

DoD contracts must also require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

Contractors shall report to the DOD each cyber incident that affects unclassified controlled technical information residing within or transiting contractor information systems in accordance with DFARS clause 204.7304 and 252.204-7012. Detailed reporting criteria and requirements are set forth in the clause at 252.204-7012, safeguarding of unclassified controlled technical information. For information on handling CUI see DODI 5200.48.

Controlled Unclassified Information (CUI) associated with this contract must be safeguarded to prevent unauthorized public disclosure. CUI such as Security Classification Guides (SCG), and other technical information with Distribution Statements B, C, D, E or F 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 must be appropriately marked and digitally signed and encrypted if being transmitted. All transmissions to personal email accounts (AOL, GMAIL, 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.
CUI Courses and Resources Created for Industry:
The Center for Development of Security Excellence (CDSE) has developed an eLearning course titled "DoD Controlled Unclassified Information (CUI) Training For Contractors (IF141.06.FY21.CTR) or the training can be taken on TWMS.
Additionally, CDSE has a CUI Toolkit available at https://www.cdse.edu/toolkits/cui/current.html. The Toolkit includes training, policy documents, resources, and an FAQ video.
Review the DoD CUI Registry at https://www.dodcui.mil to become familiar with CUI organizational index groupings and CUI categories.
Policy documents addressing CUI oversight: Do DI 5200.48 "Controlled Unclassified Information. "(https ://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF)
32 CFR 2002 Part IV National Archives and Records Administration 32 CFR Part 2002 "Controlled Unclassified Information" (https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf)
E.O. 13556 Vol 75, No 216. "Controlled Unclassified Information" (https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-283 60. pdf)
NIST Special Publication 800-171 Rev. 3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (https://csrc.nist.gov/pubs/sp/800/171/r3/final).

11.m See Specific-On-site Attachment for reporting, security, and training requirements such as contractors performing on classified contracts are required to attend Counterintelligence (CI) training annually IAW DoDD 5240.06 (Counterintelligence Awareness and Reporting (CIAR)).

Other Comments:
Ref 10k Other:
1) NS=SCI/JWICS/SIPRnet and 2) NATO awareness for SIPRnet access at government site

Ref 11M
See Specific On-Site attachment for reporting, security, and training requirements.

No further entries on this page.

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
CSM - COR Christina Nuibe	Digitally signed by: nuibe.christina.1231795819 Date: 2026.05.20 16:52:00

	NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
	Contracting officer Magda Velarde	Digitally signed by: velarde.magda.v.1398093484 Date: 2026.05.20 17:23:11
	OPSEC, RTP/SCRM Program Manager Cassidy Robertson	Digitally signed by: robertson.cassidy.ann.1548163095 Date: 2026.05.20 17:47:05
	SECURITY SPECIALIST LUIS TORRES	Digitally signed by: torres.luis.alberto.1251082576 Date: 2026.05.21 18:01:18
	Personnel Security Specialist Mary Anne Sarmiento	Digitally signed by: sarmiento.mary anne.m.1284377962 Date: 2026.05.21 18:04:22
	GSSO or , IRC & SPO, Code 874, NIWC Pacific approval for admin changes Beverly Ellis	Digitally signed by: ellis.beverly.joyce.1167033799 Date: 2026.05.26 16:40:23
	Head, IRC and Special Project Office, Code 874, NIWC Pacific Kathy Steffel	Digitally signed by: steffel.kathy.j.1098188700 Date: 2026.05.26 17:34:36

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.)*

Personnel Security Program Requirements are attached and must be passed to subcontractors.
Personnel Security Program Requirements for Unclassified/Position of Trust (POT) Contractors and Must be Passed Down to Subcontractors.
Specific On-Site Security Requirements are Attached. This document contains reporting, security, and training requirements. For authorized visits to other U.S. Government activities, the contractor must comply with all On-site Security requirements of the Host Command.
Intelligence Information attachment
Operations Security (OPSEC) requirements attached and must be passed to all Subcontractors.
Understanding OPSEC The OPSEC Cycle Bulletin 2 dated January 2023
Release of Sensitive Compartmented Information (SCI) Intelligence Information to U.S. Contractors.

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.)*

CSO and inspection authority for SCI is NAVWAR SIO. See attached SCI Addendum. DCSA is relieved of security inspection responsibility for all SCI material. DCSA retains oversight/inspection responsibilities for facility requirements and collateral information outside of Navy facilities.

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

a. GCA NAME	c. ADDRESS *(Include ZIP Code)*	d. POC NAME
Naval Information Warfare Center (NIWC) Pacific	Code 22530 53560 Hull Street San Diego, CA 92152-5001	Jose Neto
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*		**e. POC TELEPHONE** *(Include Area Code)*
N66001		(619) 368-7466
		f. EMAIL ADDRESS *(See Instructions)*
		jose.m.neto.civ@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)* Verna Minard	**d. AAC OF THE CONTRACTING OFFICE** *(See Instructions)* N66001	**h. SIGNATURE** Digitally signed by: minard.verna.f.1072405818 Date: 2026.05.26 20:10:55
b. TITLE Security Specialist	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions)*	
c. ADDRESS *(Include ZIP Code)* Naval Information Warfare Center (NIWC) Pacific 53560 Hull Street San Diego, CA 92152-5001	**f. TELEPHONE** *(Include Area Code)* (619) 553-3005 **g. EMAIL ADDRESS** *(See Instructions)* verna.f.minard.civ@us.navy.mil	**i. DATE SIGNED** *(See Instructions)* 20260526

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

- [x] **a. CONTRACTOR**
- [ ] **b. SUBCONTRACTOR**
- [x] **c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR**
- [ ] **d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION**
- [x] **e. ADMINISTRATIVE CONTRACTING OFFICER**
- [x] **f. OTHER AS NECESSARY**

(If more room is needed, continue in Item 13 or on additional page if necessary.)

Collateral COR, email: howard.l.dyckman.civ@us.navy.mil
SCI COR, email: clemente.d.rivetti.civ@us.navy.mil
SCI ACOR/CSM, email: christina.nuibe.civ@us.navy.mil
CS, email: magda.v.velarde.civ@us.navy.mil
Security, email: NIWC _PAC_ SecurityCOR@us.navy.mil