

**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:
20220531

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**

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 DUE DATE** *(YYYYMMDD)*
N00164-22-9-J004

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

- a. ORIGINAL** *(Complete date in all cases.)* **DATE** *(YYYYMMDD)*
20220316
- 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

National Security Technology Accelerator (NSTXL)
S. Tryon ST STE 1000
Charlotte, NC. 28281-0001

b. CAGE CODE

88H13

c. COGNIZANT SECURITY OFFICE(S) (CSO)

(Name, Address, ZIP Code, Telephone required; Email Address optional)
Virginia Beach Field Office (IOFSV)
277 Bendix Rd
Virginia Beach, VA 23452
Phone: 919-337-9820

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)*

Add Row

Remove last Row

Delete All Rows

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.)*

Add Row

Remove last Row

Delete All Rows

a. LOCATION(S) *(For actual performance, see instructions.)*

TBD

b. CAGE CODE

(If applicable, see Instructions.)

TBD

c. COGNIZANT SECURITY OFFICE(S) (CSO)

(Name, Address, ZIP Code, Telephone required; Email Address optional)
TBD

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

It is anticipated that this project will receive proposals from vendors that may propose deliverables ranging from Unclassified all the way through TS/SCI. The government would like to accept potential solutions at any and all of these levels. Expectation is that respondents will need to be cleared at the appropriate level aligning to their proposed deliverables. Contract language and proposals are intended to be at the unclassified level.

Department of Defense (DoD) 5G users need insight and awareness regarding the security status of existing 5G networks and local radio frequency (RF) emitters they encounter around the world. We envision a solution that possesses the capability to detect and warn the user of situations having the potential to compromise the security of the user, device or data. For example, a 5G device may be vulnerable to network behaviors that can potentially expose data, persona and/or other identifying or significant information.

Preferred solutions address all of the below requirements and specifications. Proposed solutions should address as many of the below requirements and specifications as possible.

Requirements:

- 1) The envisioned solution shall be capable of running on a UE/device and support up to 3GPP (3rd Generation Partnership Project) Rel 16. Moreover, the application must operate in both Standalone (SA) and Non-Standalone (NSA) 5G network configurations as well as support features such as sidelink, non-3GPP access (e.g., WLAN/Wi-Fi). The application must provide capabilities when the device is operating 4G, LTE configurations, 3G, and some limited support for 2G.
- 2) The solution shall provide continuous situational awareness in the device's operating area. Situational awareness shall include:
 - a) identifying potential 3G, 4G, and 5G networks as well as other wireless communications such as WIFI and Bluetooth.
 - b) identifying potential RF emitters that have the potential to compromise the security of the user, device or data.
- 3) Once the device has registered with a serving network, the solution shall detect and warn the user of situations that have the potential to compromise the security of the user, device or data. The solution should detect and identify anomalous behaviors occurring on the serving network that might indicate surveillance or intrusive actions. This specifically includes behaviors across ALL architectural partitions of the serving network, comprising RAN, Non-3GPP Access (e.g., WLAN/WIFI), Core Network and Data Network domains (including 3rd party service platforms residing in external Data Networks).
- 4) Anomalous behaviors that must be detected include, but are not limited to, attempts to download malware onto the device, attempts to modify device settings, unauthorized exfiltration of device data (rogue uploads), handover to unauthorized towers, redirection to Non-3GPP access (e.g., WLAN/WIFI), operation of the camera, and anomalous and/or unusual control messages.
- 5) If the device changes from the serving network to a different network (e.g., the device roams onto another MNO), the application must detect the change and update accordingly.
- 6) The solution should assume the device may be operating on an adversarial, untrusted Core/RAN network and must identify and mitigate risks related to control plane attempts to exploit any information on the device or the device itself.
- 7) Based on the issues identified on the serving network, the solution will enforce a reduced set of features, services, applications and/or communication modes, increasing security of the user during device operations.

Specifications:

- 1) Operating Environment
 - a. The objective is for an application that works on a 5G 3GPP Rel 16 or later Android or iOS capable device. Other less acceptable thresholds include jail broken or similar phones or non-phone hardware with reasonable size, weight, and power.
 - b. Application must work on both the UEs home network and when roaming.
 - c. Local environment scanning must include spectrum sensing functions in threat representative bands of interest.
 - d. The solution should be prepared to obtain an Interim Authority to Test (IATT) as defined in the DoD's Risk Management Framework (RMF). The solution should complete appropriate phases of DoD's Cyber Developmental Testing & Evaluation policies and guides. Reference documents are listed below.
- 2) Identification and Warnings
 - a. Application must detect and report network changes or threats within an objective of 1 second or less acceptable threshold of under 10 seconds.
 - b. Application must be able to detect anomalous behaviors from RF emitting devices including, but not limited to, incidental radiators, unintentional radiators, intentional radiators, industrial/scientific/medical equipment and equipment operating in licensed radio services. The objective is to maximize detection leveraging hardware internal to a device. The threshold allows for additional hardware integrated with a device.
 - c. Application must communicate to the user the local environmental issues that have the potential to compromise the security of the user, device or data (such as remote improvised explosive devices (IEDs), unmanned aerial vehicles (UAVs), command and control (C2) links for controlled devices, etc.).
 - d. False positive warning messages must be minimized with an objective of 5% false positive rate and a threshold of 10%.
- 3) User Interface Requirements
 - a. Alerts issues that have the potential to compromise the security of the user, device or data.
 - b. Alerts are based on the threats detected, and thresholds can be adjusted by the user.

c. Application must include a graphical user interface with control functions to allow both manual and automatic scanning and threat reporting

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 DoDM 5200.01, Volume 4 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)*
The Contracting Officer's Representative (COR) or appropriate channels.

Public Release Authority:
-----PUBLIC RELEASE OF SCI IS NOT AUTHORIZED-----

13. SECURITY GUIDANCE

Add Signature	Remove last Signature	Delete All Signatures
---------------	-----------------------	-----------------------

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.)

Estimated Completion Date of this Contract is 05/30/2024.

Reference 10b and d - Restricted Data (RD) and Formerly Restricted Data (FRD): Contractor will receive and come into contact with RD and FRD on classified capabilities, operational and technical performance specifications, parameters and test data. RD/FRD information will be handled and controlled in accordance with the requirements of the NISPOM. Contractor is permitted access to RD/FRD in performance of the contract. RD/FRD access requires a final U.S. Government clearance at the appropriate security level prior to access to RD/FRD. The highest level of classification is SECRET, with access requirements to program related information. Program related accesses, however, will require Contractor employees to have a current T5. FRD access is handled in the same manner as NSI. A written request by the Prime Contractor to the GCA Contracting Officer is required for the flow down of information to a subcontractor for FRD. Upon receiving a written request

from a Prime contractor, the GCA Contracting Officer will provide written concurrence or non-concurrence for the request of flow down FRD to the NSWC Crane Industrial Security Department.

Reference 10e(1) - Sensitive Compartmented Information:

a. Reference attached Navy SCI Addendum of Sep 2020 and item 14. Intelligence Information, TS/SCI: SCI requirements are hereby authorized. Questions regarding Item 10e (1) and requests for retention or release of intelligence shall be through the Office of Naval Intelligence NAVSEA 00G (NSWC CRANE SIO/SSO) at (812-854-1099).

b. SECNAV S4200.35A "Sensitive Activity and Intelligence-Related Contracting (SAIRC) Within the Department of the Navy of 2 Oct 19.

Reference 10g - North Atlantic Treaty Organization (NATO) Information:

Access up to NATO SECRET is authorized for this contract. Protection of NATO information shall be in accordance with USAAN 01-07 and its applicable enclosures. Access to NATO requires a final US Government National Security Clearance and must have a NATO security briefing from the FSO. A written request by the Prime Contractor to the GCA Contracting Officer is required for the flow down of information to a subcontractor for NATO. Upon receiving a written request from a Prime contractor, the GCA Contracting Officer will provide written concurrence or non-concurrence for the request of flow down NATO to the NSWC Crane Industrial Security Department. A copy of the request from the Prime contractor and the written concurrence or non-concurrence from the GCA Contracting Officer must be sent to the NSWC Crane Industrial Security Department who will then issue out the approval for flow down of NATO.

Reference 10h - Foreign Government Information (FGI):

Foreign Government Information is limited to Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, Montenegro, and North Macedonia. Special attention should be paid to 32 CFR Part 117 (NISPO), Subsection 117.14, paragraphs (1) - (p). Access to FGI requires a final U.S. Government personnel security clearance at the appropriate level.

The Contractor will require access to foreign government information in performance of this task and shall protect such information per the guidance provided by the Task Sponsor.

-Access to FGI does not include NATO information.

-Access to FGI will be provided by the Task Sponsor. The Contractor shall protect such information pursuant to the guidance received from the Task Sponsor and authority granted by the originating government.

A written request by the Prime Contractor to the GCA Contracting Officer is required for the flow down of information to a subcontractor for FGI. Upon receiving a written request from a Prime contractor, the GCA Contracting Officer will provide written concurrence or non-concurrence for the request of flow down FGI to the NSWC Crane Industrial Security Department.

A copy of the request from the Prime contractor and the written concurrence or non-concurrence from the GCA Contracting Officer must be sent to the NSWC Crane Industrial Security Department who will then issue out the approval for flow down of FGI.

Reference 10j and 111 - Controlled Unclassified Information (CUI)

DoD Instruction 5200.48 Controlled Unclassified Information (CUI), effective 6 March 2020. It is emphasized that CUI information may not be transmitted via unprotected systems, unless fully encrypted to current DoD standards. CUI shall not be released to the public without written approval from the GCA per the Defense Federal Acquisition Regulation Supplement clause 252.204-7000. All Controlled Unclassified Information (CUI) associated with this contract must be safeguarded to prevent unauthorized public disclosure. CUI such as FOUO, 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. Any CUI provided to the Contractor will be marked in accordance with DOD Instruction 5200.48 Controlled Unclassified Information (CUI), effective 6 March 2020. DoD Instruction 5200.48 supersedes DoD Manual 5200.01, Volume 4, DoD Information Security Program: Controlled Unclassified Information, February 24, 2012, as amended. All emails containing such information or attachments, shall be protected per NIST SP-800-171. 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.

Contractors receiving, transmitting or accessing controlled unclassified technical 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. Contractors shall report to the DOD each Cyber incident that affects unclassified controlled technical information resident on 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. NIST Special Publication 800-171 will be used as the Risk Management Framework for Protecting CUI and Controlled Defense Information in Nonfederal Systems and Organizations for this contract.

Reference 11a:

Access at the actual work/performance location will include the generation, management, and dissemination of classified information. All classified work will be completed at the location(s) identified in Item 8a.

Reference 11j - OPSEC:

11(j): The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSW Crane Critical Information List (CIL), NSW Crane Note 3070.1 CIL is identified under separate cover, is For Official Use Only and shall be handled as such.

11(j) Performance under this contract requires the contractor to adhere to OPSEC requirements. OPSEC requirements are additional to the requirements of 32 CFR Part 117, National Industrial Security Program Operating Manual, therefore, the Contractor may not impose OPSEC requirements on its subcontractors unless NSW Crane approves the OPSEC requirements. The contractor shall assign an OPSEC point of contact for this contract at no additional cost to the Government. This individual may be the Facility Security Officer (FSO).

11(j) During the period of this contract, the Contractor may be exposed to, use, or produce, NSW Crane Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSW Crane CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI).

11(j) Communications and electronic emails shall be encrypted and protected when containing NSW Crane CI. The transfer of unclassified technical data to and from the government or other associated activities must be accomplished via encrypted email or DoD SAFE at <https://safe.apps.mil/> or DODIIS DOTS <https://dots.dodiiis.mil/webtransfer/#/>. *Not approved for U-NNPI

11(j) Assembled large components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer. Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible.

11(j) CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be protected per NIST SP-800-171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations.

11(j) NSW Crane 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 NSW Crane Public Release Authority listed in Item 12 of this DD Form 254.

11(j) Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other programs must be immediately reported to the Facility Security Officer and Defense Counterintelligence and Security Agency and/or the Naval Criminal Investigative Service, and the NSW Crane Industrial Security Department.

11(j) NSW Crane employed contractors will be OPSEC briefed by their assigned FSO if working off site and if working on site will be briefed by their assigned directorate OPSEC program manager/coordinator on the Commands OPSEC requirements.

11(j) For specific OPSEC requirements, Critical Information Lists (CILs) and assistance contact the respective government program manager or COR.

11(j) A written request by the Prime Contractor to the GCA Contracting Officer is required for the flow down of information to a subcontractor for OPSEC. Upon receiving a written request from a Prime contractor, the GCA Contracting Officer will provide written concurrence or non-concurrence for the request of flow down OPSEC to the NSW Crane Industrial Security Department. A copy of the request from the Prime contractor and the written concurrence or non-concurrence from the GCA Contracting Officer must be sent to the NSW Crane Industrial Security Department who will then issue out the approval for flow down of OPSEC.

Questions concerning these requirements shall be directed to the NSW Crane Industrial and Operations Security POC's.

Reference 11k - Defense Courier Service:

Only certain classified information qualifies for shipment by DCS. Prior approval of GCA is required before a Prime Contractor can authorize a subcontractor to use the services of USTRANSCOM's Defense Couriers. Upon receiving a written request from a Prime contractor, the GCA Contracting Officer will provide written concurrence or non-concurrence for the request of the use of the Defense Courier Service to the NSW Crane Industrial Security Department.

A copy of the request from the Prime contractor and the written concurrence or non-concurrence from the GCA Contracting Officer must be sent to the NSW Crane Industrial Security Department.

Contractor performance shall be in accordance with 32 CFR Part 117 (NISPOM) and DFARS 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting, 48 CFR 52.204-2 - Security Requirements and NIST Special Publication 800-171. The contractor shall limit requests for Personnel (Security) Clearances (PCL) to the minimal number of personnel for operational efficiency, consistent with contractual obligations and other requirements of the NISPOM.

This DD254 and the 32 CFR Part 117, National Security Program Operating Manual (NISPOM) are part of the contract. The contractor agrees to provide and maintain a system of security controls within its own organization according to the NISPOM. All contractor personnel will obtain and maintain the appropriate level of security clearance eligibility or access as required to perform on the level of

tasking assigned. Access to classified information will be limited by the access level showing in JPAS or subsequent system of record and need to know. All classified information shall be handled in accordance with approved security practices and procedures. Contractor personnel in contact with classified documentation, information and/or equipment shall have the proper level of access showing in JPAS or the subsequent system of record and have a need to know.

Per the DFARS clause 252.204-7000:

a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

(2) The information is otherwise in the public domain before the date of release; or

(3) The information results from or arises during the performance of a project that involves no covered defense information (as defined in the clause at DFARS 252.204-7012) and has been scoped and negotiated by the contracting activity with the contractor and research performer and determined in writing by the contracting officer to be fundamental research (which by definition cannot involve any covered defense information), in accordance with National Security Decision Directive 189, National Policy on the Transfer of Scientific, Technical and Engineering Information, in effect on the date of contract award and the Under Secretary of Defense (Acquisition, Technology, and Logistics) memoranda on Fundamental Research, dated May 24, 2010, and on Contracted Fundamental Research, dated June 26, 2008 (available at DFARS PGI 204.4 (DFARS/PGI view)).

(b) Requests for approval under paragraph (a)(1) shall identify the specific information to be released, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the Contracting Officer at least 10 business days before the proposed date for release.

(c) The Contractor agrees to include a similar requirement, including this paragraph (c), in each subcontract under this contract. Subcontractors shall submit requests for authorization to release through the prime contractor to the Contracting Officer.

This clause shall also be made available to Subcontractors.

All classified information received is the property of the US Government. Any classified information generated in the performance of this contract shall be classified according to the markings shown on the source material as well as the applicable security classification guide (SCG). In the event of a discrepancy between source material and the SCG, the SCG shall prevail. Classified information shall be processed for appropriate disposition per 32 CFR Part 117 (NISPOM).

Security classification guides (OPNAVINST 5513 series) and controlled unclassified information (CUI) (e.g., FOUO, distribution statement controlled) are not authorized for public release; therefore, they cannot be posted on a publicly accessible web-server or transmitted over the internet unless appropriately encrypted. Request for public release cannot be transmitted via the internet until the contractor receives final approval from NSWC Crane PAO listed in Block 12.

Classified or unclassified technical papers to be presented at a classified symposium must be approved by the NSWC Crane Contracting Officer's Representative (COR) prior to the presentation.

All contractor requests for sharing of classified and other sensitive information between prime contracts must be forwarded in writing to the NSWC Crane Industrial Security Department.

All classified documents must be destroyed using a National Security Agency (NSA) approved high security crosscut shredder listed on the NSA/CSS evaluated products list(EPL) for high security crosscut paper shredders, or other approved method for destroying classified information.

Cleared DoD contractors shall not release intelligence to any of their components or employees not directly engaged in providing services under the contract or other binding agreement or to another contractor (including subcontractors) without the consent of the releasing command.

Cleared DoD contractors who employ foreign nationals or immigrant aliens shall obtain approval from the Director, ONI (ONI-5), before releasing intelligence to them, whether or not there is a Limited Access Authorization in place.

All classified information involved in security incidents shall be retained and provided to the certifying official in Block 17 of this DD-254 for classification review.

All reports of contractor security violations associated with this contract shall be sent by the DCSA field office directly to the certifying official in Block 17 of this DD-254.

All security related issues, requests, or incidents pertaining to this contract shall be submitted in writing by the contractor's Facility Security Officer (FSO) to the individual identified in Block 17 of this DD-254. The contractor shall abide by other reporting requirements outlined in the NISPOM.

Copies of any and all subcontract DD Form 254s shall be provided to the NSWC Crane Industrial Security Department.

Per the requirements stated in 32 CFR Part 117, National Industrial Security Program Operation Manual (NISPOM), the Facility Security Officer (FSO) on the prime contract is authorized to flow down access to each subcontractor. It is the prime contractor FSO's responsibility to ensure that all subcontractors have the appropriate access levels. It is also the prime contractor FSO's responsibility to ensure that they have documented paperwork for each subcontract. If the current prime contractor FSO is replaced, it is the responsibility of the new FSO to inform NSWC Crane in writing to Security and the COR.

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 biennial training during the life of this contract. Evidence of completion, training certificates or equivalent, shall be provided to the Information Assurance Manager no later than the individual's due date.

Visit requests to activities, other than those listed in the Statement of Work or this DD-254 shall have "Need to Know" certified by the Program Manager. All requests shall contain the information required by the NISPOM and shall not exceed a 12-month period. All visit requests to Military Installations for classified or unclassified visits from subcontractors will be sent via the prime contractor who will certify the need-to know.

All Government Badges issued under this contract will be returned immediately to the NSWC Crane Security Manager or COR upon termination of contract, or individual terminations. When an individual contractor is terminated, for any reason, it is the responsibility of the Facility Security Officer to immediately notify the Command Security Manager, 300 Hwy 361, Bldg 2, Crane, IN 47522. Failure to comply could result in the suspension of all contractor proximity key and NT accounts.

If additional contracting requirements exist where retention of classified information by the contractor facility is required, a written request to retain material for a period but not to exceed 2 years is required to the individuals listed in Blocks 16 and 17.

Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified information to the source from which received unless retention or other disposition instructions are authorized by NSWC Crane.

FAR CLAUSE - 52.204-2 -- Security Requirements

(a) This clause applies to the extent that this contract involves access to information classified "Confidential," "Secret," or "Top Secret."

(b) The Contractor shall comply with --

(1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (32 CFR Part 117); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(c) 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.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph.

The Security Classification Guide listed in Block 13 or subsequent revisions apply to this contract. Subsequent revisions shall be provided by the Government Contracting Activity as Government Furnished Information and shall be executed by the Contractor at no additional cost to the government.

Contractor employees occupying sensitive positions requiring access to classified information or CUI, whether embedded within the command or working from another location, require, at a minimum, a favorably-adjudicated T3 background investigation providing national security eligibility or an interim (temporary) national security eligibility, commensurate with contract requirements, prior to being afforded access to classified information or CUI.

SECURITY CLASSIFICATION GUIDANCE:

The following Security Classification Guide(s) apply to classified performance on this contract. Subsequent updates shall be provided by the Technical Point of Contact/Contracting Officer Representative/Contracting Officer Security Representative (as applicable) as Government Furnished Information (GFI) and shall be executed by the Contractor without obligation to modify this DD-254:

A preliminary draft 5G to NextG Systems Security Classification Guide (SCG) will provide instructions and guidance on the classification information involved in DoD 5G and NextG Systems.

SOLICITATION:

This DD254 is for solicitation purposes only; therefore it must be returned to the NSWC Crane Industrial Security Department to be updated before the contract DD254 can be issued to the contractor.

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

Add Attachment

View Selected Attachment

Remove Selected Attachment

NAME & TITLE OF REVIEWING OFFICIAL

SIGNATURE

Blake Martindale
NSWC Crane Deputy SSO

NAME & TITLE OF REVIEWING OFFICIAL

SIGNATURE

Lada Ly
NSWC Crane SSO

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
Michael B. Foster NSWC Crane SIO	
NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
Edward T. Bareng NSWC Crane COR	

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.)*

The attached Navy SCI Addendum provides the necessary guidance for physical, personnel, information and information systems security measures and is part of the SCI security specifications for the contract.

Access to intelligence information requires a special briefing and a final U.S. Government clearance at the appropriate level for access. Foreign nationals are prohibited from access to any classified information.”

DoD M-5105.21 Volumes 1-3 and effective BANIFs and NISPDs for SCI Security.

OPSEC requirements are imposed on this task. Refer to Item 13 of this DD Form 254 for applicable guidance. These OPSEC requirements cannot be imposed on subcontractors without written consent from the NSWC Crane OPSEC Program Manager. These requirements shall not be imposed at an additional cost to the government.

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.)*

Collateral Security Cognizance - DCSA
SCI Security Cognizance - SSO

NSWC CRANE DIVISION SIO has exclusive security responsibility for SCI classified material released or developed under this contract. DCSA is relieved of security inspection responsibility for all SCI material. DCSA retains oversight/inspection responsibilities for facility clearance requirements and collateral information outside of Navy facilities.

DCSA is relieved from security/inspection responsibilities for all classified material. The CSO for those locations as identified by the program manager and approved by the COR has oversight for all classified material. Security Officers onboard the designated ships and/or installations will maintain control of the classified information and conduct security inspections if required.

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

a. GCA NAME NSWC CRANE	c. ADDRESS (Include ZIP Code) NSWC Crane 300 Highway 361 Crane, IN 47522	d. POC NAME Edward Bareng
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE (See Instructions) N00164		e. POC TELEPHONE (Include Area Code) +1 (812) 854-5131
		f. EMAIL ADDRESS (See Instructions) edward.t.bareng.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) FOSTER, MICHAEL B.	d. AAC OF THE CONTRACTING OFFICE (See Instructions) N00164	h. SIGNATURE
b. TITLE NSWC CRANE SIO	e. CAGE CODE OF THE PRIME CONTRACTOR (See Instructions.)	
c. ADDRESS (Include ZIP Code) NSWC Crane 300 Highway 361 Crane, Indiana 47522-5001	f. TELEPHONE (Include Area Code) +1 (812) 854-6309	i. DATE SIGNED (See Instructions)
	g. EMAIL ADDRESS (See Instructions) michael.b.foster7.civ@us.navy.mil	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

a. CONTRACTOR

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

b. SUBCONTRACTOR

c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR

d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION

e. ADMINISTRATIVE CONTRACTING OFFICER