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: May 31, 2022

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See Instructions)*	b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY
Secret	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** N00164-21-9-W007 **DUE DATE** *(YYYYMMDD)* 20210930

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

- ☒ **a. ORIGINAL** *(Complete date in all cases.)* **DATE** *(YYYYMMDD)* 20210120
- ☐ **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)*
National Security Technology Accelerator (NSTXL) 3140 Mantle Ridge Dr. Apex, NC 27502	88H13	Virginia Beach Field Office 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)*

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		TBD

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

The Government requires a suite of T&E ready simulators for threat exploitation and countermeasure development that have been fully documented, verified, validated, and accredited. Prototype simulators will be sufficiently documented to allow routine replication of the prototypes in response to run capacity requirements. Given the increasing rate of threat development, in order to maintain robust protection of our aircraft and aircrews, the Government requires support for prototype HITL simulator development. The desired end-state objective of this RFS is to have one or more Performers fully integrated in all aspects of HITL simulator development with the Government. Below, the various phases of HITL simulator development are outlined.

The Government projects that up to 25 simulators may be required in the next 10 years. These 25 simulators will each be distinct and represent different threat missiles. Both the Government and the Performer will collaborate on the development of all future simulators;

however, individual phases may be performed by either entity or both together. For each prototype simulator development, Performer assistance may be needed for some phases and not others, itemized Performer cost estimates are requested for each of the seven phases described below. The cost for a Performer doing all the development for a given prototype simulator will be the total of the itemized costs for the seven phases. The Government may award contracts to one or more Performers.

With the posting of this RFS and upon request from the vendor, the Government will provide a classified annex that contains a list of threat missiles that are candidates for prototype HITL simulators to be developed during performance of this action. This list will be comprehensive but not all-inclusive. Development of prototype HITL simulators may be requested for threats that are not on this list. This list will be classified and will only be provided to vendors that possess the appropriate facility and personnel security clearances (details are provided below under Section 8). The Government will be requesting firm-fixed pricing for each phase (as identified below) for three (3) of the threats on the list. The three threats to be used for pricing will be clearly identified on the classified list.

Project award(s) may be for any number of prototype HITL simulator development phases, from one (1) to all seven (7). The Government is interested in potentially awarding individual projects for individual phases and groups consisting of multiple phases. For example, a missile threat could be provided to a vendor and that vendor requested to perform Phases 4-7. In that scenario, Government Furnished Information would be provided to that vendor relative to work and data gathered by the Government during Phases 1-3.
It is requested that each vendor specifically identify the length of validity of their firm-fixed pricing for the three (3) threats identified.

Phase 1 – Design

All prototype HITL simulators developed under this RFS will utilize the Reconfigurable Signal-Injection Missile Simulation (RSIMS) architecture. Depending on the specific requirements for each threat, modifications or enhancements to RSIMS may be required and are included as part of this phase (where needed). System design includes (but is not limited to) the following activities: configuration of RSIMS threads, development of subsystem models (e.g. gyroscope, reticle processor, missile airframe model, etc.), configuration of RSIMS input/ output (both digital and analog), and seeker interface and power requirements. Design documentation will be provided at the end of this phase and will include the items discussed above.

Phase 2 – Subcomponent Development

Prototype HITL simulator subcomponents must be developed. This includes development of all-digital models for the gyroscope and missile flyout, as well as hardware subcomponents like the seeker interface circuitry and computer boards.

An essential component of the development of these prototype simulators is a capability to acquire and test multiple alternative prototype simulator subcomponents. This project will require timely response by the Performer to satisfy prototype simulator subcomponent requirements. These requirements typically include, but are not limited to:

• Custom printed circuit boards (PCBs)
• Circuit Design, Fabrication, and Testing Services and Equipment
• Analog-to-Digital, Digital-to-Analog, and Digital Input/Output (IO) Cards
• GPU Cards
• FPGA Cards
• High Performance multicore computer systems and the necessary support equipment including but not limited to desktop workstations, digital simulation network servers, peripherals, and stand-alone HITL simulator systems
• Software Development Tools
• 3D printing and/or additive manufacturing of prototype designs

The development of each subcomponent will be documented in sufficient detail to produce additional copies or make design changes.

Phase 3 – Subcomponent Integration & Testing

Once the prototype simulator subcomponents have been developed, they must be integrated together and tested. This testing will be performed at the contractor's facility. Typically this is done in an incremental process where baseline RSIMS operation (stand-alone) is demonstrated first, then each all-digital subcomponent model is added one at a time, culminating in integration of the missile hardware. Incremental system testing then proceeds until the full capabilities have been demonstrated (e.g. missile flyout with image based aircraft scenes and both expendable and laser-based countermeasures).

An integration/testing report will document the results of this phase.

Phase 4 – Integration with MOSAIC GUI

In order to make the prototype simulators ready for countermeasure technique development production runs, each simulator must be integrated with the MOSAIC graphical user interface (GUI). MOSAIC (MOdular System for the Advanced Investigation of Countermeasures) is a comprehensive threat engagement modeling system developed by the Air Force Research Laboratory (AFRL). NSWC Crane uses the MOSAIC GUI to set up countermeasure effectiveness simulation runs for the threat models native to MOSAIC and our RSIMS HITL simulators. MOSAIC can be provided to the Performer as GFE.

A report will be provided by the Performer detailing modifications made to MOSAIC and the prototype HITL simulator during this phase. Digital copies of all supporting computer files will be provided by the Performer.

Phase 5 – Verification & Validation (V&V)

Verification is the process of assuring that model implementation is consistent with the intended model design. Validation is the process of assuring that a given model accurately responds the same as the real-world system that it represents. Prototype simulator V&V will be patterned after existing threat missile simulator V&V documents from other DoD facilities. Standard V&V documents from the Defense Modeling and Simulation Organization (DMSO) may also be used as templates. Certain V&V tests will be common to all threat missile simulators, but each simulator will also have unique V&V requirements identified during the process of system exploitation.
At the end of this phase, a formal V&V report will be provided.

Phase 6 – Delivery of Final Prototype HITL Simulator and Technical Data Package

Final delivery of the prototype HITL simulator will involve acceptance testing to insure proper functionality in all system modes. The technical data package will contain all design information necessary to support and/or duplicate the simulator, as well as the V&V documentation. Acceptance testing will include (but is not limited to):

- Flyout simulation runs against benign targets
- Flyout simulation runs against targets employing expendable countermeasures
- Flyout simulation runs against targets employing directed infrared countermeasures (DIRCM)
- Simulation runs in lab-bench mode
- Simulation runs in captive flight test mode (seeker test van)
- Demonstration of MOSAIC GUI integration including run set-up, execution, scoring, and post-processing (detailed performance/signal analysis), and batch run capability
- Recreation of selected parameter tests from the V&V documentation

Phase 7 – Accreditation

Each prototype simulator must be accredited for use by one or more programs. Major accreditation agencies include NAVAIR PMA-272 for developmental testing and Commander Operational Test and Evaluation Force (COMOPTEVFOR) for operational testing. Simulators may also be accredited by individual program offices, or other DoD services.

This process includes development by the Performer of an accreditation support package which includes the V&V reports as well as other documentation including configuration management, system maintenance and development.

This phase includes all activities leading to a successful accreditation, including development of the accreditation support package and reviews by various subject matter experts.

The project is expected to have a duration of 10 years. Multiple prototype HITL simulators will be developed over this period of performance.

The success criteria is delivery of a fully functional prototype HITL simulator with complete documentation and V&V report that has been accredited for use by at least one project office.

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 GOVERMENT 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)*	**Public Release Authority:**
NSWC Crane Commanding Officer Attn: PAO 300 Highway 361 Crane, Indiana 47522	Pamela Ingram-Public Affairs Officer 1-812-854-3239, pamela.ingram@navy.mil

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.)

Reference 10j and 11l: DoD Instruction 5200.48 Controlled Unclassified Information (CUI), effective 6 March 2020. All CUI information may not be transmitted via unprotected systems, unless fully encrypted using Department of Defense Public Key Infrastructure (PKI), or an approved DoD External Certificate Authority, in accordance with Public Key Infrastructure & Public Key Enabling, DoDI 8520.02, 24 May 2011. 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 in accordance with DFARS 252.204-7012 per NIST SP-800-171 rev 2. 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 or sanitize 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; or methods in accordance with DFARS 252.204-7012.

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.

Reference 11c: The Contractor requires access to classified source data up to and including the level identified in item 1a of this DD 254. Classified material generated in support of this contract shall be classified in accordance with the source material of the Navy Security Classification Guidance, which will be provided by the GCA. Automated Information Systems (AIS) must be certified and accredited by the Cognizant Security Agency prior to processing classified information.

Reference 11g: The contractor must prepare and forward DD Form 1540 to the NSWC CRANE Contracting Officer for endorsement and submission to DTIC. The contracting officer will certify the field of interest relating to the contract. DD Form 2345 must be submitted directly to the Defense Logistics Services Center for access to unclassified military critical technical data (after registration with DTIC) from DoD sources. The GCA must certify the need-to-know to DTIC.

Reference 11j:
11(j): The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSWC Crane Critical Information List (CIL), NSWC Crane Note 3070.1 CIL is identified under separate cover.
11(j) Performance under this contract requires the contractor to adhere to OPSEC requirements. OPSEC requirements are additional to the requirements of DoD 5220.22-M, National Industrial Security Program Operating Manual, therefore, the Contractor may not impose OPSEC requirements on its subcontractors unless NSWC 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). A facility level OPSEC is required.
11(j) During the period of this contract, the Contractor may be exposed to, use, or produce, NSWC Crane Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSWC 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 NSWC Crane CI per guidance provided for item 11(l) of this DD Form 254. The transfer of unclassified technical data to and from the government or other associated activities must be accomplished via encrypted email per NIST SP 800-171 or DoD SAFE at https://safe.apps.mil/ or DODIIS DOTS https:// dots.dodiis.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) NSWC 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 NSWC 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 and electronic spillage of government Classified or CI related to this contract must be immediately reported to the Facility Security Officer and Defense Security Service and/or the Naval Criminal Investigative Service, and the NSWC Crane Industrial Security Department. All instances of loss or compromise of controlled unclassified information shall be reported per requirements of DFARS 252.204-7012(c).
11(j) NSWC 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 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 OPSEC.

Contractor performance shall be in accordance with the NISPOM, DoD 5220.22-M, February 28, 2006, Change 2 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 DOD-5220.22 M Change 2, May 2016, 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 DoD 5220.22-M (NISPOM), chapter 5, section 7.

Security classification guides (OPNAVINST 5513 series) and controlled unclassified information (CUI) (e.g., FOUO, distribution statement controlled) is not authorized for public release; therefore, they cannot be posted on a publicly accessible web-server or transmitted over the internet unless appropriately encrypted per guidance provided for item 11(l) of this DD Form 254. 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 the National Industrial Security Program Operation Manual (NISPOM) dated February 2006, Chapter 5,

Section 5, Paragraph 5-502, 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 (DoD 5220.22-M Change 2); 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:

Applicable Security Classification Guides to the work that will be performed and will be used to determine appropriate levels for subject data marking, storage, and dissemination:
Issued by Defense Intelligence Agency (executive agent); Missile and Space Intelligence Center (MSIC), National Air and Space Intelligence Center (NASIC), National Ground Intelligence Center (NGIC), Office of Naval Intelligence (ONI), and the U.S. Army Program Manager for Short and Intermediate Effectors for Layered Defense (PM SHIELD) are the overall project executives:
• ASCOT DAZZLE SCG, 15 Mar 2012,
• ASCOT EAGLE SCG, 2 Feb 2012,
• ASCOT FALCON SCG, 6 Aug 2004,

- ASCOT FORGE SCG, 13 Oct 2009,
- ASCOT LURE SCG, 2 Feb 2012,
- ASCOT SHALE SCG, 19 May 2009,
- ASCOT SLIDE SCG, 30 Aug 2012,
- ASCOT WALTZ SCG, 10 Aug 2005,
- ASCOT WREN SCG, 15 Mar 2012,
- DROVE ATLAS SCG, 8 Oct 2006,
- DROVE BISALT, 14 May 2014,
- DROVE CRADLE SCG, 16 Jan 2009,
- DROVE SPORT SCG, 21 Mar 2005,
- GRAY ROCK SCG, 2 May 2005,
- IBIS BORAX SCG, 17 Nov 2011,
- MOBIUS TALENT, 13 Nov 2017,
- PROJECT KHUZI, 31 Oct 2016
- Stinger Based Systems SCG, Cruise Missile Defense Systems, 17 March 2012.

SOLICITATION:
This DD254 is for solicitation purposes only; therefor 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)

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
Dave Robertson NSWC Crane OPSEC Manager	ROBERTSON.DAVID.LEE.1081503784 Digitally signed by ROBERTSON.DAVID.LEE.1081503784 Date: 2021.01.22 09:55:36 -05'00'

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.)*

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.)*

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

a. GCA NAME	c. ADDRESS *(Include ZIP Code)*	d. POC NAME
NSWC Crane	NSWC Crane 300 Highway 361 Crane, IN 47522	Brent Waggoner
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*		**e. POC TELEPHONE** *(Include Area Code)*
N00164		+1 (812) 854-3939
		f. EMAIL ADDRESS *(See Instructions)*
		brent.waggoner@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)*	
Miller, Jason M	
b. TITLE	
Security Contracting Officer	

c. ADDRESS *(Include ZIP Code)* NSWC Crane Division 300 Highway 361 Crane, Indiana 47522	**d. AAC OF THE CONTRACTING OFFICE** *(See Instructions)* N00164 **e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)*	**h. SIGNATURE** MILLER.JASON.MICHAEL.1259557298 Digitally signed by MILLER.JASON.MICHAEL.1259557298 Date: 2021.01.22 09:59:12 -05'00' **i. DATE SIGNED** *(See Instructions)* 20210122
	f. TELEPHONE *(Include Area Code)* +1 (812) 854-2147 **g. EMAIL ADDRESS** *(See Instructions)* jason.m.miller5@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.)*