CLASSIFICATION *(When filled in)*: [redacted]

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
Top Secret	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)*

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

- ☒ **a. ORIGINAL** *(Complete date in all cases.)* **DATE** *(YYYYMMDD)*
- ☐ **b. REVISED** *(Supersedes all previous specifications.)* **REVISION NO.** **DATE** *(YYYYMMDD)*
- ☐ **c. FINAL** *(Complete Item 5 in all cases.)* **DATE** *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☒ No ☐ Yes *If yes, complete the following.*

Classified material received or generated under _____ *(Preceding Contract Number)* **is transferred to this follow-on contract.**

5. IS THIS A FINAL DD FORM 254? ☒ No ☐ Yes *If yes, complete the following:*

In response to the contractor's request dated _____ **, retention of the classified material is authorized for the period of:** _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
		Defense Counterintelligence & Security Agency Alexandria Field Office IOFCS1 DSS.Alexandria1@mail.mil 571-551-7920

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)*
Performance on this contract is restricted to government facilities in the National Capital Region (NCR)		

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

Provide specialized and sensitive administrative, security, operations, policy, and analytic support to the Influence and Perception Management Office (IPMO) in the Office of the Under Secretary of Defense for Intelligence and Security OUSD(I&S).

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
- [redacted] 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.)*

NIPRNet, SIPRNet, JWICS, PDAS, SIC accounts

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

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

Courier authorization

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:**
Public release of SCI/Non-SCI information is not authorized unless granted by written approval from OUSD(I&S).	Defense Office of Prepublication and Security Review and/or SSO DIA

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 FSO/AFSO shall immediately report to the COR, but no later than 24 hours from discovery, all security incidents. A security incident may be an infraction or violation. The FSO/AFSO shall forward all final incident reports to the COR for concurrence; this is in addition to the NISPOM reporting requirements to DCSA, when applicable.

All security requirements contained within this DD Form 254, where applicable, shall be applicable to any subcontractors and consultants supporting this contract. Subcontracting approval is required.

REQUIRED CLEARANCE LEVEL This contract involves access to classified data/information up to and including TOP SECRET/SCI. All contractor personnel performing under this contract shall possess the appropriate interim or final clearance prior to reporting to any assignment.

NON-DISCLOSURE AGREEMENT (CNSI & CUI) All contractor personnel performing under this contract shall be required to sign and execute proprietary information non-disclosure statements for Classified National Security Information (CNSI). The proprietary

information non-disclosure statements shall be required as part of the initial in-processing and must be executed prior to performing any work under this contract. Contractor personnel who refuse to sign proprietary information non-disclosure statements will not be permitted to work on government contracts.

SECURITY EXECUTIVE AGENT DIRECTIVE 3 The contractor must comply with "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position," along with DoD Manual 5200.02 and NISPOM.

SECURITY EXECUTIVE AGENT DIRECTIVE 4 The contractor will comply with "National Security Adjudicative Guidelines," which became effective on June 08, 2017. See INDUSTRIAL SECURITY LETTER (ISL) 2019-01 for additional information.

ORIGINAL CLASSIFICATION AUTHORITY Original Classification is not authorized. If the contractor believes information not currently classified, requires classification, the contractor will immediately notify the GCA.

SECURITY CLASSIFICATION GUIDANCE (SCGs) Specific SCGs, to include subsequent upgrades/revision(s), applying to classified performance on this contract, shall be provided by the Contracting Officer Representative or Technical Point of Contact, identified in Block 16, as Government Furnished Information (GFI); and shall be executed by the Contractor without obligation to modify this DD Form 254. If additional security classification is required, contact the COR identified in Block 16.

TELEWORK If approved to telework, use of classified information is prohibited. Unclassified information and CUI must be accessed via Government approved equipment and DoD network. Personal software/equipment must not be introduced/connected to DoD equipment or used to process DoD information. Connection of personal devices to a DoD computer is prohibited.

DESTRUCTION OF DoD INFORMATION The contractor must comply with on-site security procedures to dispose of DoD Information.

DISPOSITION OF DOD INFORMATION & EQUIPMENT All information/equipment must be returned to the Government when no longer required for performance on this contract.

AUDIO/VISUAL RECORDINGS The recording of DoD information, equipment, personnel, or facilities by any means is prohibited.

SECURITY INCIDENTS The contractor will immediately report to the GCA any known or suspected incident in which government information/equipment is not properly safeguarded or has been disclosed to unauthorized persons; electronic data spills on information systems; or concerns of workplace violence.
- Notify the Facility Security Officer (FSO)
- Notify the GCA security office as appropriate (Government Security Manager).
- For PFPA: Industrial Security Program Manager, 703-697-5113 Office, 571-429-2306 Cell, pfpa.ncr.ssd.mbx.industrial-security@mail.mil
- For WHS Security Office: Whs.pentagon.em.mbx.security-officers@mail.mil, or 571-372-0921/0938/0936/0940.
- For Electronic Spillage, Notify the FSO, Security Manager and PENTCIRT immediately: Hotline (703) 695-CIRT(2478) to report data spills. Initial report should be UNCLASSIFIED.
- Law Enforcement needed: Notify the Pentagon Force Protection Agency: Emergency: 703.697.5555 or 911 from Office Landline; Non-Emergency Phone: 703.697.1001

COMPUTER SECURITY Contractor personnel are "Authorized Users" of the DoD networks and must comply with responsibilities identified in DoDI 8500.01. Contractor "Privileged User" access must be specifically authorized, otherwise the contractor will not have access to system control, monitoring, administration, criminal investigation, or compliance functions unless specifically authorized. Contractor personnel must:
- Comply with laws, rules, and regulations for use of information systems.
- Meet all requirements before accessing a particular information system.
- Use information systems only for the official purpose specified in this contract.
- Not process classified information on unclassified systems or systems of a lower classification.
- Complete mandatory initial and annual cyber awareness training.
- Complete Privacy Act training.
- Enforce need to know.
- Not share system access tokens (e.g. CAC) or passwords, with other individuals.
- Follow procedures to address suspicious email (e.g. phishing).
- Not introduce personal wireless hot spots or portable electronic devices (e.g. cell phone) into spaces where classified or sensitive information is processed/stored.
- Not post DoD information to publicly accessible web sites.
- Not process DoD information on personal devices (e.g. cell phone, laptop, camera, voice recorders).
- Not use thumb drives or other storage devices.

- Not introduce or use software, firmware, equipment, hardware, or USB devices, to the DoD network that has not been approved by the Government Network Authorizing Official (Defense Information Systems Agency/Joint Service Provider).
- Not connect any personal devices/equipment to DoD equipment/network.
- Not connect Government issued equipment (e.g. local desk top printer; government issued iPhone) before obtaining approval from the information system owner.
- Return Government equipment when no longer required for performance on this contract.

ADDITIONAL SECURITY REQUIREMENTS FOR PERFORMANCE IN GOVERNMENT FACILITIES The contractor will comply with site specific security procedures and complete required security training. Additional security requirements may be by the Department Of Defense imposed during the contract.

MOBILE DEVICES (Prohibited Electronic Devices (PEDs)) The introduction of mobile devices (personal or government issued) into facilities where classified information is processed, handled, stored, or discussed, is prohibited. Prohibited devices normally feature the ability to receive or transmit data, record audio/video, make cellular phone calls, and have Wi-Fi technology. Examples of prohibited devices include but are not limited to: cell phones; laptops; smart watch; camera; MP3 player. Key fobs for medical alert, motor vehicle, or home security are generally acceptable provided they have no features similar to prohibited devices. Medical devices may be acceptable but require individual assessment.

SAFEGUARDING CLASSIFIED INFORMATION & CUI DURING MEETINGS and/or PRESENTATIONS Classified information must be protected from unauthorized disclosure. Classified meetings/training/conferences (presentations) must be pre-approved by the GCA; must serve a specific U.S. Government purpose; dissemination of classified information by other means is not sufficient; must take place only at an approved U.S. Government facility or cleared contractor facility meeting appropriate safeguard requirements. The contractor must comply with all safeguarding requirements during classified presentations. Classified presentations at non approved Government locations (e.g. hotel) is prohibited. CUI must be protected from unauthorized disclosure. CUI presentations must be pre-approved by the GCA and must serve a specific U.S. Government purpose. CUI presentations must take place at Government approved locations and must not occur in locations where there is risk of unauthorized disclosure to foreign personnel/governments or others who do not have an official "need to know." For additional information refer to the NISPOM, DoDM 5200.01 Volumes 1 through 3 and DoDI 5200.48.

10.a. COMSEC information. Classified COMSEC material is not releasable to contractor employees who have not received a final security clearance at the appropriate level. Cryptologic keying materials and Controlled Cryptographic Items (CCI) are controlled by Department of Defense, NISPOM, and National Security Agency (NSA) guidelines. The contractor shall be guided by NSA/CSS Policy Manual 3-16 in the control and protection of COMSEC material/information at their facilities. When access is required at Government facilities, contractor personnel will adhere to COMSEC rules and regulations as mandated by DoD 5520.22-M, EKMS 1 (series), Command policy and procedures. Written concurrence of the Technical Point of Contact (TPOC) identified in Block 16, or Contracting Officer Representative/ Contracting Officer Representative (COR) for Security (as applicable) is required prior to subcontracting IAW 32 CFR Part 117 NISPOM 117.21 (h).

10e(1): SCI Requirement. The Director, DIA has exclusive security responsibility for SCI released or developed under this contract. The COR shall ensure contractors under this project are appropriately cleared in accordance with Security Executive Agent Directive (SEAD) 4, dated June 8, 2017, or successor documents, and the contractor must agree to follow controls and procedures for SCI protection, handling, and accountability. Performance requiring access to or at the SCI level shall be governed by the SCI addendum titled "Release Of Sensitive Compartmented Information (SCI) Intelligence Information To Us Contractors". Access to Intelligence information requires a final Top Secret U.S. Government clearance and SCI indoctrination. Contractor will require access to ICD 703 and ICD 710. The names of contractor personnel requiring access to SCI shall be submitted to the contracting officer's representative (COR) for approval. The COR will approve and coordinate visits by contractor personnel to insure satisfactory justification. Prior approval of GCA is required for subcontracting.

All activities involving SCI (including discussions) shall be conducted in Sensitive Compartmented Information Facilities (SCIFs). The contractor shall adhere to all physical security standards for SCIFs as described in ICD/ICS 705.

The contractor is not authorized to further disclose or release classified national intelligence and SCI (including to a subcontractor) without prior written authorization of the originating IC element in accordance with 32 CFR Part 117, NISPOM.

10e(2): Non SCI Intelligence. Performance requiring access to Non-SCI intelligence information shall be governed by the addendum titled "Release of Non-SCI Intelligence Information to DoD Contractors" Contractor will require access to ICD 503. Prior approval of GCA is required for subcontracting.

10.f. Special Access Provisions Apply. Contract requires access to Special Access Programs (SAP). All SAP material remains the property of the Government Contracting Activity (GCA) and is considered non-releasable. Upon completion or cancellation of this contract, the government Program Security Officer (PSO) will provide specific direction regarding the disposition of SAP materials received or

generated under the contract. The SAP PSO or Program Manager will provide security classification guidance for the performance of the contract. Contractor personnel must adhere to the special access security classification and SAP procedural guidance provide for programs or studies. SAP access must be requested by a person knowledgeable of the activity and approved by a designated access approval authority. Public release of information related to this activity is not permitted. Contact the PSO for any request for release of information. Prior approval of GCA is required for subcontracting. Security policy for the protection of SAP information will follow the provisions of DoD Directive 5205.07, Special Access Program Policy, and DoD Instruction 5205.11, Management, Administration, and Oversight of DoD SAPs, including associated DoD Manuals 5205.07, Volumes 1 through 4, and applies on all OUSD(I&S) SAP efforts.

10.g. NATO Information. To facilitate potential access to NATO classified information, to include NATO accredited SIPRNet terminals, all DoD military, civilian, and contractor personnel who are briefed on their responsibilities for protecting U.S. classified military information, shall also be briefed on the requirements for protecting NATO information, per Deputy Under Secretary of Defense Policy Security Memo of 5 Dec 01. Written concurrence of the Contracting Officer/Technical Point of Contact, identified in Block 16, is required prior to subcontracting IAW 32 CFR Part 117, NISPOM 117.19(g(9). The briefing form is located here: https://www.cdse.edu/documents/toolkits-fsos/NATO_Brief.pdf.

10h: Foreign Government Information is information provided to the U.S. by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information or both, are to be held in confidence; or produced by the U.S. pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence. Access to FGI requires a final U.S. Government clearance at the appropriate level. Comply with the Foreign Government information requirements in the NISPOM, Chapter 10, section 3. Prior approval of GCA is required for subcontracting IAW 32 CFR Part 117 NISPOM 117.17 (a)(3)(iv).

10.j. CUI Information. Controlled Unclassified Information including Covered Defense Information (meeting the definition of 48 CFR 252.204-7012(a)) generated and/or provided under this contract shall be marked and safeguarded as specified in DoD Instruction 5200.48 Controlled Unclassified Information (CUI). Any product containing Covered Defense Information shall be assigned the appropriate distribution statement using the criteria set forth in DoDI 5230.24 Distribution Statements on Technical Documents. All Covered Defense Information (CDI), and program Controlled Unclassified Information (CUI) data transmitted and safeguarded via electronic means shall use approved encryption. The Freedom of Information Act applies.

10.k. Other: Common Access Cards. This contract requires personnel to obtain the Government issued Common Access Card (CAC) in order to provide identification for access to government computer systems and physical access to facilities. Personnel must meet and maintain investigative and adjudicative requirements specified in DoDI 5200.46, and immediately report to the GCA any issues affecting CAC eligibility. Government issued credentials are the property of the United States Government and must be returned when no longer required for performance on this contract. Return CACs to: OUSD(I&S) Security Office. CACs will not be used to access information systems, facilities, or installations that are outside the performance requirements of this contract. CACs will be used only by the individual to whom it was issued and will not be used for or by any other person. The contractor will immediately notify the GCA if a CAC is lost, stolen, or otherwise missing. Replacement CACs will require the contractor employee to obtain a signed memo from the OUSD(I&S) Security Office, requesting a new CAC be issued.

10.k. Other: NIPRNET access required. This contract requires the contractor to access and use the Unclassified government computer system known as the NIPRNET at locations identified by the government customer. All provisions of DoD Risk Management Framework (RMF) apply. This system is Unclassified only, and inappropriate or improper use of the system will result in a reportable incident to the DCSA. NIPRNET as well as other unclassified systems or equipment (e.g. printers, facsimile) will not be used to process classified information. NIPRNET systems will be used only for an official Government purpose. Inappropriate or improper use of the NIPRNET system will result in a reportable incident to the Defense Counterintelligence and Security Agency (DCSA).

10.k. Other: SIPRNET access required. This contract requires the contractor to access and use the Classified government computer system known as the SIPRNET at locations identified by the government customer. All provisions of DoD Risk Management Framework (RMF) apply. This system is authorized for use to but not exceeding the Secret-level only, and inappropriate or improper use of the system will result in a reportable incident to the Defense Counterintelligence and Security Agency (DCSA).

DERIVATIVE CLASSIFICATION training is required as a condition of access to SIPRNET. The contractor will maintain training certificates and provide copies to the GCA when requested. Annual training is required.

10.k. Other: JWICS access required. This contract requires the contractor to access and use the Classified government computer system known as the Joint Worldwide Intelligence Communication System (JWICS) at locations identified by the government customer. All provisions of DoD Risk Management Framework apply. This system is authorized for use up to but not exceeding the Top Secret level only, and inappropriate or improper use of the system will result in a reportable incident to the Defense Counterintelligence and Security Agency (DCSA).

10.k Other: SAP Network access required. This contract may require access to the Secure Integrated Cloud (SIC) and Planning and Decision Aid System (PDAS) at locations identified by the government customer. All provisions of DoD Risk Management Framework apply.

11.a. Have access to classified information ONLY at another contractor's facility OR at a government activity. If block 11a. is checked, blocks 11b., 11c., 11d., 11h., 11.i. and 11k. shall not be checked. Check block 11.a. yes if the contractor WILL NOT receive or store classified at their facility. When block 11.a. is checked, block 8.a. must identify all actual U.S. Government work location(s); block 1.b. would be marked NONE. All classified information/material shall be provided by the contractor facility or Government Contracting Activity (GCA) and safeguarded at the approved actual performance site.

11.j. Operations Security. Checking block 11.j. indicates additional OPSEC requirements above the requirements of the NISPOM.

11.m. Courier authorizations. This contract requires personnel to obtain the Government issued Courier Authorization DD-2501 or letter; couriers must complete required training; double lockable courier bags or equivalent will be used; travel via aircraft is prohibited; classified information will not be viewed during transit; couriers will use the most direct routes to the approved destination; couriers will report any failure to safeguard classified information to their FSO and GCA Security Manager. All contractor courier personnel are required to in-process with the Security Office to obtain courier cards. All personnel issued Courier Cards are required to ensure the card is returned to the Security Office or the CAC Coordinator upon removal from the contract or termination of employment under this contract.

11.m. Performance as Activity Security Representatives. Contractor may require performance as an alternate Activity Security Representative. Responsibilities of the Office Security Manager are available in the OUSD(I&S) Security and SAPCO offices and must be adhered to.

11.m. IT Operation and Support Positions. Contractor will require access to sensitive unclassified government automated information systems (AIS) at different levels. Contractor must comply with DoDI 8500.01 Cybersecurity.

CUI REQUIREMENTS FOR DOD CONTRACTORS

The following procedures will be used to protect Controlled Unclassified Information (CUI) documents and materials:

1) HANDLING: Access to CUI material shall be limited to those employees needing the material to perform their duties. The CUI marking is assigned to documents and material created by a DoD User Agency. CUI is not a classification, but requires extra precautions to ensure it's properly safeguarded and disseminated and is not released to the public without government authorization.

2) MARKING: Mark unclassified documents containing CUI: "CUI" at the top and bottom of each page, include the CUI warning box, and the CUI Designation Indicator Block as required in DoDI 5200.48. In a classified document:

a) Mark individual paragraph containing only CUI, but not classified material by placing "(CUI)" at the beginning of the portion.

b) Mark top and bottom of each page with classified material with the highest security classification of the material on the page.

c) If the document or material contains CUI under the category of Controlled Technical Information (CTI), use of distribution statements is required. See DoDI 5200.48.

d) If a classified document contains CUI material or if the classified material becomes CUI when declassified, place the following statement on the bottom of the cover or the first page under the classification marking: "NOTE: If declassified, review the document to make sure the material is not still CUI. If it does, then it must have the appropriate safeguarding, dissemination controls, and CUI markings applied.

e) Mark other records such as computer print outs, photographs, films, tapes, or slides in accordance with DoDI 5200.48 so the receiver or viewer knows the it contains CUI material.

f) Mark a message containing material in accordance with DoDI 5200.48. Unclassified messages containing CUI material must show the abbreviation (CUI) before the text begins.

g) Ensure documents transmitting CUI material call attention to any attachments containing CUI.

h) CUI material released to a contractor by a DoD user agency must have the following statement on the front page or cover:

THIS DOCUMENT CONTAINS CUI MATERIAL AND MUST BE REVIEWED BY A GOVERNMENT REPRESENTATIVE UNDER THE REQUIREMENTS OF DODI 5200.48, DODI 5230.09, and DODI 5230.29.

3) STORAGE: During normal duty hours, place CUI material in an out-of-sight location if your work area is accessible to persons who do not have an authorized government purpose for access to the material. After normal duty hours, store CUI material to prevent unauthorized access. File with other unclassified records in unlocked files or desks when internal building security is provided and the file is marked as CUI. When there is no internal security, locked buildings or rooms usually provide adequate after hours protection. For additional protection, store CUI material in locked containers such as file cabinets, desks, or bookcases. Expenditure of funds for security containers or closed areas solely for the protection of CUI material is prohibited.

4) TRANSMISSION: CUI documents and materials may be transmitted via first class mail, parcel post or for bulky shipments-fourth class mail. Within the CONUS discussion of CUI material on the telephone is authorized if necessary for the performance of the contract and no alternative is available. Electronic transmission of CUI (voice, data, or facsimile) should be by approved secure communications systems whenever practical. If there is a fax transmission, the sender must ensure the intended receiver is available to receive it or a cover sheet will be used to allow carrying it to the final recipient to avoid unauthorized disclosure of the CUI.

5) RELEASE: CUI material shall not be released outside of the contractor's facility except to the representative of DoD.

6) DESTRUCTION: When the CUI material no longer meets the threshold for safeguarding and dissemination, it shall be immediately decontrolled, be processed through the records management process, and destroyed by the approved methods identified in DoDI 5200.48 precluding its disclosure to unauthorized individuals by rendering it unreadable, indecipherable, and irrecoverable.

RELEASE OF NON-SCI INTELLIGENCE INFOMRATION TO DOD CONTRACTORS

1) Requirements for access to non-SCI:

a) All intelligence material released to the contractor remains the property of the US Government and may be withdrawn at any time. Contractors must maintain accountability for all classified intelligence released into their custody.

b) The contractor must not reproduce intelligence material without the written permission of the originating agency through the DIA/SSO. If permission is granted, each copy shall be controlled in the same manner as the original.

c) The contractor must not destroy any intelligence material without advance approval or as specified by the contract monitor (CM). (EXCEPTION: Classified waste shall be destroyed as soon as practicable in accordance with the provisions of the Industrial Security Program).

d) The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need to know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the CM.

e) The contractor must ensure each employee having access to intelligence material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody.

f) Intelligence material must not be released to foreign nationals or immigrant aliens whether they are consultants, US contractors, or employees of the contractor and regardless of the level of their security clearance, except with advance written permission from the originator. Requests for release to foreign nationals shall be initially forwarded to the contract monitor and shall include:

i) A copy of the proposed disclosure.

ii) Full justification reflecting the benefits to US interests.

iii) Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient.

g) 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 intelligence (furnished or generated) to the source from which received unless retention or other disposition instructions (see 32 CFR Part 117 (NISPOM) Rule) are authorized in writing by the CM.

h) The contractor must designate an individual who is working on the contract as custodian. The designated custodian shall be responsible for receipting and accounting for all classified intelligence material received under this contract. This does not mean that the custodian must personally sign for all classified material. The inner wrapper of all classified material dispatched should be marked for the attention of a designated custodian and must not be opened by anyone not working directly on the contract.

i) Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency through the contract monitor unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the CM for this contract in writing and must clearly indicate the justification for retention and identity of the specific document to be retained.

j) Classification, regrading, or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the contract monitor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified.

2) Intelligence material carries special markings. The following is a list of the authorized control markings of intelligence material:

a) "Dissemination and Extraction of Information Controlled by Originator (ORCON)." This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used on intelligence which clearly identifies, or would reasonably permit ready identification of an intelligence source or method which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item or information will reasonably be protected by use of other markings specified herein, or by the application of the "need-to-know" principle and the safeguarding procedures of the security classification system.

b) "Authorized for Release to (Name of Country(ies)/International Organization." The above is abbreviated "REL _____." This marking must be used when it is necessary to identify classified intelligence material the US government originator has predetermined to be releasable or has been released through established foreign disclosure channels to the indicated country(ies) or organization.

3) The following procedures govern the use of control markings.

a) Any recipient desiring to use intelligence in a manner contrary to restrictions established by the control marking set forth above shall obtain the advance permission of the originating agency through the CM. Such permission applies only to the specific purposes agreed to by the originator and does not automatically apply to all recipients. Originators shall ensure that prompt consideration is given to recipients' requests in these regards, with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

b) The control marking authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form) with data stored or processed in automatic data processing systems. The control marking also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control marking applies to several or all portions, the document must be marked with a statement to this effect rather than marking each portion individually.

c) The control markings shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other marking specified by E.O. 13526 and its implementing security directives. The marking shall be carried forward to any new format in which the same information is incorporated including oral and visual presentations.

d) Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the DIA/ SSO. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirements and copies of the DD Form 254 and Statement of Work.

RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI) INTELLIGENCE INFORMATION TO US CONTRACTORS

SCI BILLETS AUTHORIZED: ( )
Note: Names are not required. SSO will validate that contractors request for # of SCI access/read-ins do not exceed the number listed above.

1) Requirements for access to SCI:

a) All SCI will be handled in accordance with special security requirements, which will be furnished by the designated responsible special security office (SSO).

b) SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.

c) Names of contractor personnel requiring access to SCI will be submitted to the contract monitor (CM) for approval. Upon receipt of written approval from the CM, the company security officer will submit request(s) for special background investigations in accordance with the NISPOM, to the DIA/SSO. The entire personnel security questionnaire package should not be forwarded to the DIA/SSO. The Contractor Special Security Officer (CSSO) must follow the instructions provided by the DIA/SSO to the CSSO.

d) Inquiries pertaining to classification guidance on SCI will be directed through the CSSO to the responsible CM as indicated on the DD Form 254.

e) SCI furnished in support of this contract remains the property of the Department of Defense (DoD) department, agency, or command originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed IAW instructions outlined by the CM.

f) SCI will be stored and maintained only in properly accredited facilities at the contractor location.

2) The contract monitor (CM) will:

a) Review the SCI product for contract applicability and determine that the product is required by the contractor to complete contractual obligations. After the CM has reviewed the SCI product(s) for contract applicability and determined that the product is required by the contractor to complete obligations, the CM must request release from the originator through the DIA/SSO. Originator release authority is required on the product types below:

i) Documents bearing the control markings of ORCON, PROPIN.

ii) GAMMA controlled documents.

iii) Any NSA/SPECIAL marked product.

iv) All categories as listed in DoDM 5105.21-M-1.

b) Prepare or review contractor billet/access requests to insure satisfactory justification (need-to-know) and completeness of required information.

c) Approve and coordinate visits by contractor employees when such visits are conducted as part of the contract effort.

d) Maintain records of all SCI material provided to the contractor in support of the contract effort. By 15 January (annually), provide the contractor, for inventory purposes, with a complete list of all documents transferred by contract number, organizational control number, copy number, and document title.

e) Determine dissemination of SCI studies or materials originated or developed by the contractor.

f) Within 30 days after completion of the contract, provide written disposition instructions for all SCI material furnished to, or generated by, the contractor with an information copy to the supporting SSO.

g) Review and forward all contractor requests to process SCI electronically to the accrediting SSO for coordination through appropriate SCI channels.

h) Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the DIA/SSO. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirement and copies of the DD Form 254 and Statement of Work.

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**

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE

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 contractor shall abide by the requirements in Intelligence Community Directive (ICD) 701, December 17, 2017, or its successor document, for any suspected or actual unauthorized disclosures in addition to the requirements in 32 CFR Part 117, NISPOM. The ICD 701 is available at https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

The contractor shall abide by the requirements in DoDM 5105.21, Volumes 1 through 3, or successor documents, to include Intelligence Community Directives (ICD) as required by the COR in addition to the requirements in 32 CFR Part 117, NISPOM. The DoDM 5105.21, Volumes are available at http://www.esd.whs.mil/Directives/issuances/dodm/.

DoDM 5105.21, Vol 1-3, DoDM 5200.01 Vol 1-3. OPSEC in contract. GCA will provide additional security guidance as required.

SCI classified information used in this project is derivative information and shall be protected in accordance with source documents.

SCI Requirement. (Applies if 10.e.(1) is yes) Performance requiring access to or at the SCI level shall be governed by the SCI addendum titled "Release of Sensitive Compartmented Information (SCI) Intelligence Information to U's Contractors". Prior approval of contracting activity is required for subcontracting. Access to Intelligence information requires SCI indoctrination and a final Top Secret U.S. Government clearance. Contractor will require access to DCID 6/1, DCID 6/4, DCID 6/6, ICD 704 and ICD 710. The names of contractor personnel requiring access to SCI shall be submitted to the contracting officer's representative (COR) for approval. The COR will approve and coordinate visits by contractor personnel to insure satisfactory justification.

Non SCI Requirement. (Applies if 10.e.(2) is yes) Performance requiring access to Non-SCI intelligence information shall be governed by the addendum titled "Release of Non-SCI Intelligence Information to DoD Contractors" Contractor will require access to ICD 503. Access to intelligence information requires special briefings and a U.S. Government clearance at appropriate level (TS/SCI) as designated by government program manager. Prior approval of contracting activity is required for subcontracting.

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.)*

OUSD(I&S) has exclusive security responsibility for inspection of classified materials within the SCIF that are released or developed under this contract. DCSA shall have exclusive security responsibility for inspection of all collateral classified materials and information stored or processed external to the SCIF at the location identified in Item 8.a. in accordance with 32 CFR Part 117, NISPOM.

SSO DIA has exclusive security responsibility for all SCI classified material released to or developed under this contract. DSCA is relieved of security inspection responsibility for all such material. DIA is responsible for reviewing all the contract's SCIF documentation to ensure compliance with SCIF regulations. DSCA retains oversight responsibility for collateral information.

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

a. GCA NAME	c. ADDRESS *(Include ZIP Code)*	d. POC NAME
DoD/WHS/AD	4800 Mark Center Dr, Suite 09F09 Alexandria, VA 22350	Wimper, Nikita N
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*		**e. POC TELEPHONE** *(Include Area Code)*
HQ0034		+1 (703) 470-2353
		f. EMAIL ADDRESS *(See Instructions)*
		nikita.n.wimper.civ@mail.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)*	

b. TITLE	d. AAC OF THE CONTRACTING OFFICE *(See Instructions)*	h. SIGNATURE
OUSD(I&S) C&SP COR	HQ0208	
c. ADDRESS *(Include ZIP Code)* OUSD(I&S) 5000 Defense Pentagon Washington, D.C. 20301	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)*	
	f. TELEPHONE *(Include Area Code)*	**i. DATE SIGNED** *(See Instructions)*
	g. EMAIL ADDRESS *(See Instructions)*	

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.)*