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: October 31, 2020

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.)* N/A
- ☐ **b. SUBCONTRACT NUMBER** N/A
- ☐ **c. SOLICITATION OR OTHER NUMBER** **DUE DATE** *(YYYYMMDD)* N/A

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)*
N/A		DSS Field Office DSS Email Address DSS Phone #

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)*
N/A		N/A

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)*
N/A		DSS Field Office DSS Email Address DSS Phone #

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

Brief, very generic, high-level unclassified statement.

Period of Performance:

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.)*

AIS (DSWAN)

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:**
The Strategic Capabilities Office, copy to SCO PM public.release@sco.mil	The Strategic Capabilities Office 675 N. Randolph St, Arlington, VA 22203

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.)

10a; COMMUNICATIONS SECURITY (COMSEC) INFORMATION. Classified COMSEC information/material will be protected IAW DoD 5220.22-M (Ch 9, Sec 4) and NSA-CSS Policy Manual 3-16. Access to classified COMSEC information requires a final USG clearance at the appropriate level.

10b; RESTRICTED DATA (RD). Access to RD, information which is classified and controlled under the Atomic Energy Act of 1954 may be required for performance on this contract. A final U.S. Government (Top Secret or Secret) clearance is required for this project. Information in this category relates to: (1) the design, manufacture or utilization of atomic weapons, (2) the production of special nuclear material; or, (3) the use of special nuclear material in the production of energy. Information of this category shall not be disseminated outside official and authorized channels without the consent of the originator. Access to and dissemination of this information shall be governed by DoD Instruction 5210.02.

10c; CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) INFORMATION. Access to CNWDI may be required for performance on this contract. The government program manager or designated representative will brief all contractors prior to granting access to CNWDI information. Contractor must be briefed by an appropriate government agent and follow the guidelines as outline in DoD Instruction 5210.02.

10d; FORMERLY RESTRICTED DATA (FRD). Access to FRD information may be required for performance on this contract. Information that is removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For Foreign Dissemination however, it is treated in the same manner as Restricted Data. Information of this category shall not be disseminated outside official channels without the consent of the originator. Access to and dissemination of this information shall be governed by DoD Instruction 5210.02. Access to FORMERLY RESTRICTED DATA requires a final U.S. Government clearance at the (Secret or Top Secret) level.

10j; CONTROLLED UNCLASSIFIED INFORMATION (CUI). Access to CUI is required for performance on this contract. IAW DoDM 5200.01 Volume 4, EO 13556, 32 CFR Part 2002, NIST SP 800-171 Rev 1, DFAR Supplement Clause 252.204-7012 Version 2, and applicable guidance provided by the CSA, certain types of information require safeguarding or dissemination controls to ensure it is not released improperly. CUI categories include, but are not limited to: (1) Procurement and Acquisition Information (i.e., contractor proposals and source selection information), (2) Proprietary Data (i.e., information protected under the Trade Secrets Act, 18 USC §1905), (3) For Official Use Only(FOUO) Information(i.e., information that is exempt from release under The Freedom of Information Act, 5 USC §552), (4) Export Restricted or Controlled Technology (e.g., defense articles and technical data restricted by the International Traffic in Arms Regulations (!TAR), 22 CFR §§120-130), (5) Program-specific Financial Data, (6) Limited Distribution Unclassified Intelligence Information, (7) Law Enforcement Sensitive Information, (8) Personal Identifying Information (PII), (9) Critical Infrastructure, (I0) North Atlantic Treaty (NATO) Restricted or Unclassified Information, (11) DoD Unclassified Controlled Nuclear Information. At a minimum, all SCO technical program information should be marked as U//FOUO.

10k; OTHER. DSWAN ACCESS REQUIRED. Access to the DARPA Secure Wide Area Network (DSWAN) may be required for performance on this contract. All provisions of DoD Risk Management Framework (RMF) apply. DSWAN is authorized to process information up to the Collateral SECRET level (includes NOFORN and REL). NATO and SAR information is not authorized on DSWAN. Inappropriate or improper use of the system will result in a reportable incident to Defense Security Service (DSS).

11a; The contractor is only authorized to access classified information at the following locations: Company Name, Address, CAGE Code, DSS Field Office/CSO Information.

11c; RECEIVE, STORE AND GENERATE CLASSIFIED INFORMATION OR MATERIAL. Receiving, storing and generating classified information or material is required for performance on this contract. Access to classified information cannot be precluded. The contractor is not authorized to release program information to any activity or person, including subcontractors, without prior approval from SCO. Classified material generated on this contract shall be classified IAW SCO-provided classification guidance and applicable references. Automated Information Systems (AIS) must be certified and accredited by the appropriate CSA for the AIS prior to processing classified information for SCO programs. All classified information received or generated under this contract is the property of the USG.

11d; FABRICATE, MODIFY or STORE CLASSIFIED HARDWARE. Fabricating, modifying or storing classified hardware may be required for performance on this contract. The contractor must provide appropriate storage to protect hardware up to the classification level listed in Block 1b, at the location(s) listed in Block 8a.

11g; BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER. Contractor is authorized to use the services of the Defense Technical Information Center (DTIC) and is required to prepare and process DD Form 1540. Contracting Officials, with concurrence from the program manager/project manager, must review and approve contractors need-to-know and ensure all identified DTIC information requirements are within Scope of Work prior to approving the DD Form 1540. Certification of need-to-know and use of DTIC field of interest register for the acquisition of reference materials classified through Top Secret/RD, disclosures authorizations, and visits clearance approvals, fall under the responsibility of the Contract Monitor (CM).

11h; REQUIRE A COMSEC ACCOUNT. A COMSEC account is required for performance on this contract. The contractor must forward requests for COMSEC material/information through the COR, AOR, CM, CSA or equivalent. The contractor must follow all guidance in DoD 5220.22-M (Ch 9, Sec 4) and NSA-CSS Policy Manual 3-16.

11j; HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS. All organizations participating in SCO programs have an OPSEC requirement. Due to SCO's increased media attention and the high potential for adversaries to target/collect program data, properly applied OPSEC measures must be taken into account to protect sensitive unclassified information. The PM at each work location (government and industry) is responsible for the protection of both unclassified and classified SCO technical program information. The PM will: (1) Not provide any SCO technical program information (unclassified or classified) to any individual or organization (this includes periphery program support; contracts, finance, etc.), until they have read and understand program-specific security requirements (This applies only if the individual has a Need- To-Know (NTK) for technical program information for execution of their duties.

If they do not have a NTK for technical program information (e.g. - individual only requires unclassified administrative, non- technical program information, the local PM and/or designated Security POC is responsible for reviewing the administrative program information prior to release, ensuring there are no compilation concerns.), (2) Designate a Security POC and provide them the appropriate resources required to protect technical program information, (3) Strictly enforce NTK and (4) Implement OPSEC measures. Each organization is required to create a program-specific OPSEC Plan (or incorporate OPSEC into an existing plan). The PM at each work location will acknowledge their aforementioned responsibilities in the Program Partner Data Sheet.

11l; RECEIVE, STORE OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI). Receiving, storing or generating CUI is required for performance on this contract. Storage and transmission requirements set forth in (1) DoD Manual 5200.01, Volume 4; DoD Information Security Program: Controlled Unclassified Information (CUI), 24 Feb 2012, (2) Executive Order (EO) 13556, Controlled Unclassified Information, 4 Nov 2010, (3) Code of Federal Regulations Title 32 Part 2002 (32 CFR Part 2002), Controlled Unclassified Information (CUI), 14 Sep 2016, (4) NIST Special Publication 800-171 Rev I, Protecting Controlled Unclassified Information in Nonfederal Systems and Organization, updated 28 Nov 2017 (includes updates from 7 Jun 2018), (5) DFARS Clause 252.204-7012 Version 2, Safeguarding Controlled Technical Information, Aug 2015, and any other applicable guidance provided by the CSA must be adhered to. CUI must be transmitted by DoD-approved encryption software, approved secure communications systems, systems utilizing protective measures such as Public Key Infrastructure (PKI) or USPS mail.

12; PUBLIC RELEASE. All organizations participating in programs sponsored by SCO must adhere to SCO public release guidelines. Public release of information is not automatic. The fact that classified and unclassified information is in the public domain does not mean it has been officially released. All information must be protected IAW program security requirements until officially notified by SCO. Personnel must not perpetuate or further disseminate information related to program activities to the media, other organizations or to non-accessed personnel. Any contact or unauthorized release must be reported immediately to SCO Security (within 24 hours).

Proposed release of information regarding any SCO program must receive approval prior to publication or distribution. Public release includes any printed articles, company websites, advertising pamphlets, internet posting, SEC filings, information discussed in an open forum/symposium, etc. Public release requests for ANY information related to SCO programs must be submitted to SCO at least 30 days prior to requested release date. To request a public release approval, provide justification for proposed release (i.e. - what is the benefit to the USG for releasing information to the public), in addition to DD Form 1910, proposed material and partner approvals (if applicable). Submit the request to public.release@sco.mil for review.

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
Strategic Capabilities Office	Brett A. Nelson, Director, Security & Program Protection	

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 DARPA Secret Wide Area Network (DSWAN) will be operated IAW the DARPA-DSS MOU dated December 12, 2016, as amended. Data Transfers: Data transfers will be performed IAW the processes and procedures outlined in the DARPA "Data Transfer SOP," November 21, 2017, Version 1.8 (or most recent version) for accredited DSWAN systems.

COGNIZANT SECURITY AUTHORITY (CSA). The SCO Security Director is the CSA for all SCO programs that comprise the SCO portfolio, including external programs owned by other agencies/services. CSA does not transfer to the contracting agent. SCO is the CSA for all SCO concepts and funded SCO programs. SCO Security, in collaboration with industry and government partners, is responsible for ensuring physical and information security measures are implemented and maintained in areas where SCO program information (unclassified, collateral, SAP, SCI) is processed, stored, discussed, manufactured, tested or destroyed. To ensure protection measures are in place, SCO must be cognizant of all locations where SCO program work is conducted. This includes meetings held at any contractor locations that are not identified on the DD254 or Program Partner Data Sheet, and any tests/simulations/analysis, etc. that occurs outside SCO-approved program areas. All program meetings must be held in pre-approved spaces. All program participants must submit a Program Partner Data Sheet, via secure channels, prior to receiving any program information. The SCO Director, Security and Program Protection may sponsor and/or accredited SCIF/SAPF/Closed Area facilities (as required) and provide (as GFE) and/or sponsor specialized classified networks to support. The facilities must be "consolidated/contiguous" and be configured and situated in such a way to allow maximum use for all personnel on campus working/NTK on SCO efforts (company or organization wide regardless of division, group, directorate, etc).

CUI PROTECTION MEASURES. Protection measures utilized in the mitigation plan must employ at least one of the following mitigations; (1) Encryption of data at rest on unclassified servers (in addition to end-point encryption for data at rest),(2) Off-network storage/repository for data protection and segregation (e.g.-full air gapped system), (3) FOUO accredited software suite (i.e. - APAN, D2IE, TENS, etc.), (4) MS or Adobe encryption with password protection for each file (NOTE: Password cannot be sent via the same medium as the protected file. For example, if you email a password protected document on NIPR, you cannot email the password on NIPR. You must use alternate means.), or (5) an equivalent level of protection identified by the requestor. Mitigation plans must be submitted to the program PSR via secure channels for approval by the SCO Program Manager and SCO Security Director.

COMPILATION. All organizations participating in programs sponsored by SCO must protect CUI from unauthorized or inadvertent disclosure. Amassing large amounts of data/combining unclassified elements of information may increase overall classification level if compiled unclassified data reveals classified aspects. All documents and material will be classified by content. A higher classification level may be assigned if the compilation increases the overall classification level (i.e. - relationships, program sensitivities, technical aspects, payloads, etc.). Prior to forwarding or replying to emails, ensure the entire email string is reviewed for compilation issues.

UNCLASSIFIED IDENTIFIERS. Because SCO programs leverage multiple existing/fielded capabilities, they are inherently comprised of information at various levels of classification. In conjunction with horizontal protection and other employed techniques, SCO uses unique unclassified identifiers to obfuscate program information. The implementation of unique identifiers at each organization lays the appropriate foundation for executing a successful OPSEC risk mitigation plan. Unclassified identifiers are unique to an organization and/or capability. Every program partner (government and industry) must identify their own unique unclassified identifier on their Program Partner Data Sheet. If the Program Partner Data Sheet does not identify a unique, internal unclassified identifier, one will be assigned by SCO. Unclassified identifiers will be disseminated to the program team via MFR, Baseline Protection Concept and/or PSPP revision. OPSEC should be taken into consideration when selecting an unclassified identifier (i.e. - should not be related to program activities or reveal/imply the nature of the program). The unclassified identifier cannot be used for multiple programs or efforts. It must be unique and only used for this specific program. Any changes to the Program Partner Data Sheet must be submitted to the SCO PSR within 5 working days.

The association of ANY unclassified identifier with its R-2 or actual name/term/nomenclature will, at a minimum, be protected at the SECRET level. All material must be marked based on content. Classified technical program information associated with an unclassified identifier does not change the classification level of the content. Unclassified identifiers are for use in unclassified channels. Unclassified identifiers should not/are not required to be used in classified channels. Unclassified identifiers are NOT a means to "talk around" classified information.

SUBCONTRACTING. Subcontracting is only applicable to industry partners. Prior to subcontracting any SCO program work, the prime contractor must obtain written concurrence from the SCO Security Director. All SCO requirements must flow down to subcontractors and consultants. Subcontractor DD254s must be pre-approved prior to the start of any work or releasing any technical program information, regardless of classification. To obtain CSA approval for subcontractors, submit a DD254 (with SCO Security Director concurrence line in Block 13) and a completed Program Partner Data Sheet (completed and signed by the on-site POC for that location). Submit the DD254 to the PSR via unclassified channels (encrypted) and Program Partner Data via secure channels only to the program PSR for review and routing.

SECURITY INCIDENTS. SCO maintains security cognizance of all incidents regarding SCO program information. Reports of loss, compromise or suspected compromise must be reported immediately (within 24 hours) to the SCO Security Director via the Program Security Representative (PSR). Failure to comply with any security requirements or guidance (and any revisions/updates) will be construed as an item of non-compliance on performance.

CLASSIFICATION GUIDANCE. Further dissemination of technical program information must be coordinated with the CSA, or designee, prior to releasing the information (unclassified or classified) to any activity or person, including subcontractors, vendors or suppliers. The recipient must have a valid NTK for the information and must have a current DD254 with SCO language (if the recipient is a contractor) or other CSA-approved documentation (e.g. - MFR). Program participants must adhere to all current and applicable successor classification guidance provided by the CSA. SCGs, PSPPs and Baseline Protection Concepts are maintained by SCO Security and will be provided by the program PSR. All program participants will comply with all applicable guidance, as determined by the CSA. Program participants are required to comply with the spirit and intent of the PSPP. Individuals are not authorized to downgrade or change the content contained in the PSPP. SCO will provide additional security classification guidance or interpretation, as needed.

DISTRIBUTION STATEMENTS. All unclassified SCO technical program information is FOR OFFICIAL USE ONLY (U//FOUO) and must carry Distribution Statement F. "DISTRIBUTION STATEMENT F. Further dissemination only as directed by The Strategic Capabilities Office, 675 N. Randolph St, Arlington VA 22203, 28 Aug 2018." FOUO information (e.g. - data, websites, email, etc.) and material shall be transmitted by approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure (PKI). Correspondence on NIPR that contains U//FOUO material/information must be password protected and/or encrypted, must not contain information that when compiled, would reveal/imply classified technical program information, and must have an approved mitigation plan.

CLASSIFICATION DISCREPANCIES. If a discrepancy exists between SCO classification guidance and existing SCGs, protect the information at the highest classification level until the existing SCG has been reviewed for scope and applicability. Review and arbitration of conflicting guidance will be led by SCO Security. SCO Security will ensure all guidance is reviewed and de-conflicted, ensuring horizontal protection of all information. If any party witting of this effort is aware of existing classification guidance (Collateral, SAP, SCI), they are obligated to notify SCO Security immediately. At a minimum, identify the SCG, and provide CSA and GPM contact information.

COMMON ACCESS CARDS (CAC). This contract may require personnel to obtain a Government-issued CAC to access government facilities for meetings and tests (network access, OCONUS and on-site contract performance is not authorized). The SCO PM will identify the contractors requiring a CAC and provide appropriate justification to SCO Security, for submission to the SCO TASS Trusted Agent (TA). As a condition of this contract, all personnel issued a Government CAC are required to ensure the card is returned to an authorized RAPIDS location or to the SCO Security office upon removal from the contract or termination of employment. Contractor (and associated subcontractor) employees shall comply with adjudication standards and procedures; applicable installation, facility and area commander installation and facility access and local security policies and procedures (provided by Government representative); or, at OCONUS locations, IAW status-of-forces agreements and other theater regulations.

----------NOTHING FOLLOWS----------

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.)*

In accordance with the DARPA-DSS MOU, dated December 12, 2016, as amended, DSWAN is under the security cognizance of DARPA and may include visits from DARPA Security and Intelligence Directorate personnel, along with DSS representatives, to validate the secure operating status of the network.

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

a. GCA NAME N/A	**c. ADDRESS** *(Include ZIP Code)*	**d. POC NAME**
		e. POC TELEPHONE *(Include Area Code)*
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)* N/A		**f. EMAIL ADDRESS** *(See Instructions)*

17. CERTIFICATION AND SIGNATURES

Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below. Upon digitally signing Item 17h, no changes can be made as the form will be locked.

a. TYPED NAME OF CERTIFYING OFFICIAL *(Last, First, Middle Initial)* *(See Instructions)*	d. AAC OF THE CONTRACTING OFFICE *(See Instructions)*	h. SIGNATURE
Nelson, Brett		
b. TITLE	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)*	
Director, Security & Program Protection		
c. ADDRESS *(Include ZIP Code)*	**f. TELEPHONE** *(Include Area Code)*	**i. DATE SIGNED** *(See Instructions)*
675 N. Randolph St Arlington, VA 22203	+1 (703) 526-4738	
	g. EMAIL ADDRESS *(See Instructions)*	
	brett.nelson@sco.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.)*