DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: TOP SECRET

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

☐	a. PRIME CONTRACT NUMBER	
☐	b. SUBCONTRACT NUMBER	
☒	c. SOLICITATION OR OTHER NUMBER: W911W4-13-R-0005-0006	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 specs)*	Revision No.	Date *(YYYYMMDD)*
☐	c. FINAL *(Complete Item 5 in all cases)*		Date *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☒ NO. 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? ☐ YES ☒ NO. If Yes complete the following

In response to the contractor's request dated _____ , retention of the identified 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 *(Name, Address, and Zip Code)*
This DD 254 is for solicitation purposes only. A DD254 will be issued for the prime contract upon contract award.		

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICES *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Multiple Location		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Systems Integration

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☒	☐
b. RESTRICTED DATA	☐	☒
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☐	☒
d. FORMERLY RESTRICTED DATA:	☐	☒
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)	☒	☐
(2) Non-SCI	☒	☐
f. SPECIAL ACCESS INFORMATION	☐	☒
g. NATO INFORMATION	☒	☐
h. FOREIGN GOVERNMENT INFORMATION	☒	☐
i. LIMITED DISSEMINATION INFORMATION	☐	☒
j. FOR OFFICIAL USE ONLY INFORMATION	☒	☐
k. OTHER *Specify)* NIPRNET, SIPRNET, JWICS, NSANET AND ASEP ACCESS	☒	☐

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☐	☒
b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☐	☒
c. RECEIVE AND GENERATE CLASSIFIED 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 THE DEFENSE COURIER SERVICE	☐	☒
l. OTHER *(Specify).* REQUIRES SI/TK/G/& HCS ACCESSES, SEE SCI ADDENDUM	☒	☐

DD Form 254, DEC 1999 *Previous editions are obsolete*

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release

☐ Direct ☒ Through *(Specify):*

PUBLIC RELEASE OF SCI IS NOT AUTHORIZED. Request for release of other than SCI must be approved by the Contract Monitor.

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance 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 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 document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*

SEE SECTION 13 CONTINUATION SECTION AT THE BOTTOM OF THIS FORM

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(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 cognizant security office. Use Item 13 if additional space is needed.)* ☒ Yes ☐ No

SEE SCI ADDENDUM

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.* ☒ Yes ☐ No

SEE SCI ADDENDUM

16. CERTIFICATION AND SIGNATURE. 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.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Eunice "Liz" Wright	INDUSTRIAL SECURITY OFFICER	703-428-4372

d. ADDRESS *(Include ZIP Code)*

HQ USAINSCOM, ATTN: IASE-IS
8825 BEULAH STREET
FORT BELVOIR, VA 22060-5246

e. SIGNATURE

Eunice K. Wright

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
- ☒ b. SUBCONTRACTOR
- ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- ☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- ☒ e. ADMINISTRATIVE
- ☒ f. OTHERS AS NECESSARY **(CSE, CM, CSSO/FSO)**

DD Form 254 (BACK), DEC 1999

13. SECURITY GUIDANCE. The security classification guidance 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 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 document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*

10 (a): Classified COMSEC material is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. COMSEC access shall be IAW 000 5220.22-M and AR 380-40. When access is required at Government facilities, contractor personnel will adhere to COMSEC rules and regulations as mandated by Command policy and procedures. Written concurrence of the KO is required prior to subcontracting.
10e(1): SCI Access required for access to SCI networks: JWICS and NSANET and supporting intelligence databases. Written concurrence of the CM is required prior to subcontracting. No public release of information authorized, public disclosure or confirmation of any subject related to the support contract is not authorized without first obtaining written approval from the KO. The Contractor Facility Security Officer (FSO) will work with the Contract Support Element (CSE) to process requests for SCI access in ACAV and future software systems used by CSE. Contractor must notify CSE and the COR any change in status of SCI-accessed personnel: marriage, divorce, name change, etc. Contractor will inform CSE and COR within 24hrs of when they become aware of derogatory information (arrests, security incidents, etc.). Contractor will report derogatory information meeting the standards of AR 380-67 immediately as an incident report to the Joint Personnel Adjudication System (JPAS) as well as notify the Defense Security Service (DSS) in accordance with the NISPOM.
10e(2): Access to collateral intelligence information required for performance and access to SIPRNET. Non-SCI Information is not releasable to contractor employees who have not received a clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting.
10g: The SIPRNET and JWICS contain NATO information and a NATO awareness briefing is required for everyone who needs access to SIPRNET or JWICS. The purpose of providing a NATO awareness briefing is to inform personnel how to protect NATO information in the event they come across it while on the SIPRNET. See 10k below for additional information.
10h: Foreign Government Information (FGI) is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting. Exposure to FGI is based on access to SIPRNET, JWICS and NSANET networks and supporting databases.
10j: For Official Use Only (FOUO). The contractor is responsible for handling and protection of FOUO markings only when generated and disseminated by the Government, and is required to apply FOUO markings only when extracting FOUO information from such material. See Appendix A, FOUO Information. Controlled Unclassified Information (CUI) including, Law Enforcement Sensitive (LES) requires safeguarding or dissemination control. Contractor may disseminate CUI to its employees who have a valid "need to know" to support this contract. No further distribution of the information is authorized without prior approve of the COR. CUI generated and/or provided under this contract shall be safeguarded and marked as specified in DOD 5200.1, Volume 4, 24 Feb 12.
10k: NIPRNET, SIPRNET, JWICS and NSANET access required. The contractor shall not access, download or further disseminate any special access data (i.e. intelligence, NATO, COMSEC, etc.) outside the execution of the defined contract requirements and without the guidance and written permission of the KO. In the event that any special access is required, the KO must modify the requirements for the DO Form 254. All contract personnel must follow requirements in AR 25-2, Information Assurance and the INSCOM Acceptable Use Policy.
11c &d: Contractor will receive, generate, modify, and store classified material and hardware/systems only in support of INSCOM Futures mission requirements at the GSS-CGI SCIF located at 6363 Walker Lane, Suite 200 Alexandria, VA, 22310. This contract is responsible for creating a testing environment that mimics current production environments to test new products and systems prior to deployment in an operational environment.
11iTEMPEST requirements are in support SCIF regulations and policy. Requirements provided under separate cover from CM and or CSA
11j: INSCOM OPSEC Requirements provided under separate cover from CM.
11i: SI/TK/G and HCS SCI accesses required to perform work on this contract. All personnel working under this contract must be trained on Executive Order 13526. Any extracts for use of classified data requires the contractor to apply derivative classifications IAW INSCOM OPORD 11-092 and FRAGO 1. All markings must be consistent with the source documents. Contractor shall notify the COR two weeks prior to personnel leaving the contract. Contractor will inform the COR immediately when personnel are no longer employed under this contract, so their credentials (CAC Card, Security Badges, etc) are returned to the government and permission to US Government Systems is deactivated. The government reserves the right to direct any contractor employee to be removed from performance, directly or indirectly. Whenever there is probable cause to believe, on the basis of all the facts available, that such action is warranted in the interest of national security. This action shall be made whether or not the cause is deemed sufficient to warrant action to terminate the contractor's or individual's security clearance. The government also reserves the right to remove any contractor for the purpose of conducting any investigation of alleged misconduct which may, in the opinion of the Contracting Officer, jeopardize the security of the project. This DD254 has been approved by the Industrial Security Manager prior to submission in ACAVS.

W911W4-13-R-0005-0006

US ARMY SCI ADDENDUM TO DD FORM 254, 31 May 2005

XXX (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, US Anny Intelligence and Security Command (INS COM), acting on behalf of the DA Deputy Chief of Staff (DCS), G-2 as the Cognizant Security Authority (CSA) for the US Anny, has exclusive security responsibility for all SCI released to the contractor or developed under the contract and held within the Contractor's SCI Facility (SCIF) or Co-utilization Agreement (CUA) SCIF. The Defense Intelligence Agency (DIA) has security inspection responsibility for SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under the contract and held within the DoD Contractor's SCIF. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel, and information security for safeguarding SCI, and are part of the security classification specification for this contract:

XXX DoD 5105.21 -M-l, SCI Security Manual, Administrative Security

XXX Signals Intelligence Security Regulations (SISR) (Available from the CM)

XXX lmagery Policy Series (Available from the CM)

XXX ICD 703, Protecting Sensitive Compartmented Information Sources and Methods

XXX ICD 705, Sensitive Compartmented Information Facilities

XXXAR 25-2, Information Assurance

XXX AR 380-28, DA Special Security System

____ AR 380-381, Special Access Programs (SAPS).

XXX Army Handbook for SCI Contracts

XXX Other, JCD 702 Technical Surveillance Countermeasures;

XXX (2) Contract estimated completion date: _____ (NOTE: Section *"F"* of the contract normally provides the Period of Performance. Option years are not to be included, as an option is not valid until exercised by the government.)

XXX (3) The name, telephone number, email address and mailing address of the Contract Monitor (CM) for the SCI portion of this contract is:_____8825 Beulah St., Fort Belvoir VA, (Additionally, identify the Security POC & phone number and email address at the contractor's/subcontractor's location): _____ (The Contract Monitor and the contractor security must be registered in the Army Contractor Automated Verification System (ACAVS) in order to process SCI actions)

XXX (4) All DD Forms 254 prepared for subcontracts involving access to SCI under this contract must be forwarded to the CM for approval and then to HQ INSCOM, ACofS Security, 02, Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

XXX (5) The contractor will submit the request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the Contractor Support Element at least ten (10) working days prior to the visit.

XXX (6) The contractor will not reproduce any SCI related material without prior written permission ofthe CM.

XXX (7) Security Classification Guides or extracts are attached or will be provided under separate cover.

XXX (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3, and AR 25-2 (Note: Check only if item indicates that a requirement exists for SCI IS processing.)

XXX (9) This contract requires a contractor SCIF

XXX (10) This contract requires (SI) (TK) (G) (HCS) (Add others as required) (NATO SECRET) (add others as required)

XXX (1 1) The contractor will perform SCI work under this contract at the following locations: HQ INSCOM, 8825 Beulah Street, Fort Belvoir, VA 22060 and 6363 Walker Lane, Suite 200 Alexandria, VA, 22310,worldwide as required to support FUTURES mission directed by the Contract Monitor.

FOUO ADDENDUM TO DD 254

W911W4-13-R-0005-0006

SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION
(Updated: 23 July 2010)

1. The "FOR OFFICIAL USE ONLY" marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.

2. Other non-security markings such as "Limited Official Use" and "Official Use Only" are used by non-DOD User Agencies for the same type of information and should be safeguarded and handled in accordance with instructions received from such agencies.

3. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release, to determine whether a significant and legitimate Government purpose is served by withholding the information or portions of it.

4. IDENTIFICATION MARKINGS:

a. An unclassified document containing FOUO information shall be marked "UNCLASSIFIED//FOR OFFICIAL USE ONLY" in bold letters at least 3/16 of an inch high at the top and bottom of the front cover (if any), on each page, and on the outside of the back cover (if any). No portion marking will be shown.

b. Within a classified document, an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked "U//FOUO".

c. Any "FOR OFFICIAL USE ONLY" information released to a contractor by a DOD User Agency is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA. EXEMPTIONS APPLY.

d. Removal of the "FOR OFFICIAL USE ONLY" marking can only be accomplished by the originator or other competent authority. When "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent possible.

5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.

6. STORAGE: During normal working hours "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material

with other unclassified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.

7. TRANSMISSION: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent fourth-class mail. Electronic transmission of FOUO information by voice, data, facsimile or similar means, should be by approved secure communications systems when possible.

8. DISPOSITION: When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a trash container or as directed by the User Agency.

9. UNAUTHORIZED DISCLOSURE: Unauthorized disclosure of "FOR OFFICIAL USE ONLY" information does not constitute a security violation but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.