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
NONE

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-0005-0004	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 locations, see SCI Addendum		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Integrated Offensive IO Operations Intl Soulutions

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☒	☐	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☒	☐
b. RESTRICTED DATA	☐	☒	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☐	☒
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☐	☒	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	☐	☒
d. FORMERLY RESTRICTED DATA	☐	☒	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	☐	☒
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	☐	☒
(1) Sensitive Compartmented Information (SCI)	☒	☐	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	☒	☐
(2) Non-SCI	☒	☐	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	☐	☒
f. SPECIAL ACCESS INFORMATION	☒	☐	h. REQUIRE A COMSEC ACCOUNT	☒	☐
g. NATO INFORMATION	☒	☐	i. HAVE A TEMPEST REQUIREMENT	☒	☐
h. FOREIGN GOVERNMENT INFORMATION	☒	☐	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	☒	☐
i. LIMITED DISSEMINATION INFORMATION	☐	☒	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	☐	☒
j. FOR OFFICIAL USE ONLY INFORMATION	☒	☐	l. OTHER *(Specify)*.	☒	☐
k. OTHER *Specify)* NIPRNET, SIPRNET, JWICS, NSANET	☒	☐	REQUIRES SI/TK/G/& HCS ACCESSES, SEE SCI ADDENDUM		

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

This DD 254 has been approved by the INSCOM G2 SECURITY MANAGER, G3 Network Warfare Government Special Access Program Security Officer (GSSO) prior to submission in ACAVS.

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.

Eunice "Liz" Wright	Industrial Security Specialist	703-428-4372

d. ADDRESS *(Include ZIP Code)*

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

e. SIGNATURE

Eunice E. 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

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.*

10a. 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 DoD 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. 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.

10e(2) 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. Access to Intelligence information required for performance.

10f. Discussion, storage, or processing of SAP information associated with this contract will be conducted in facilities specifically accredited by the Army SAPCO (or designee), or equivalent component-level SAPCO. Contact the appropriate servicing SAPCO for approved SAP facilities locations. SAP activities are governed by Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement, 1 APR 04, and applicable program security classification and procedures guides. Component-managed SAPFs and SAP Temporary Secure Working Areas (TSWA) are governed by JAFAN 6/9. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities are under the cognizance of the SAPCO, as appropriate. Additional SAP security requirements may apply at alternate locations/facilities based on service/component Command requirements. The KO for these locations/facilities will provide specific guidance as required. SAP inspections conducted at contractor facilities are under the security oversight of the Defense Security Service (DSS) unless officially relieved of their oversight responsibilities.

10g. Personnel not assigned to a NATO staff position, but requiring access to NATO classified information, NATO COSMIC, NATO Secret or access to the NATO accredited SIPRNET terminals, must possess the equivalent FINAL or Interim U.S. Security Clearance based upon the appropriate personnel security investigation required. Personnel with access to NATO ATOMAL information must have the appropriate level FINAL U.S. Security Clearance. The government program/project manager is the designated representative that will ensure the contractor security manager and concerned employees are NATO briefed prior to access being granted. The contractor will maintain strict compliance in regards to NATO information IAW NISPOM Ch 10, Section 7. Prior approval from the KO is required for subcontracting

10h. For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD 5200.1-R, Appendix 3 (attached).

10J. 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.

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 DD Form 254.

11a. Contractor performance is restricted to U.S. government controlled and managed facilities in CONUS and OCONUS as directed by the Contract Monitor. Government agency or activity will provide security classification guidance for performance of this contract. Submit visit request via ACAVS/JPAS to the KO and/or Security Management Office or Contract Monitor for need-to-know verification.

11f. Access to classified material outside of the United States is restricted to US Government Activities only.

11l. SI/TK/G and HCS accesses required to perform work on this contract. TARP Training is required. The COR/CM/KO will ensure the contractors with security clearance comply with threat awareness and requirements specific in AR 381-12, para 1-14. Contractors will report threat-related incidents, behavioral indicators, and other matters of CI interest to their FSO (Facility Security Officer), the nearest military CI office, the Federal Bureau of Investigation (FBI) or the Defense Security Service.

W911W4-13-R-0005-0004

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 Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff (DCS), G-2 as the Cognizant Security Authority (CSA) for the US Army, 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-1, SCI Security Manual, Administrative Security
XXX Signals Intelligence Security Regulations (SISR) (Available from the CM)
XXX Imagery Policy Series (Available from the CM)
_____ ICD 703, Protecting Sensitive Compartmented Information within Information Systems
_____ ICS 705-1, Physical and Technical Security Standards for Sensitive Compartmented Information Facilities
XXX AR 25-2, Information Assurance
XXX AR 380-28, DA Special Security System
XXX AR 380-381, Special Access Programs (SAPS).
XXX Army Handbook for SCI Contracts.
_____ Other

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: Asberry, Amy E (703) 706-1846 amy.asberry@mi.army.mil 8825 Beulah St. Ft. Belvoir, VA 22060 and the alternate_____ (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, G2, 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 of the 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 11l indicates that a requirement exists for SCI IS processing.)

____ (9) This contract requires a contractor SCIF.

XXX (10) This contract requires ☒ (SI) ☒ (TK) ☒ (G) ☒ (HCS) ☒ (SAP) ☒

XXX (11) The contractor will perform SCI work under this contract at the following locations: The contractor will perform SCI work under this contract at the following locations: HQ USAINSCOM, 8825 Beulah Street Fort Belvoir, VA 22060-5246, CONUS and OCONUS U.S. controlled and managed government facilities as directed by the Contract Monitor.

W911W4-13-R-0005-0004

FOUO ADDENDUM TO DD FORM 254

SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

1. The "For Official Use Only" (**FOUO**) 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 is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (**FOIA**).

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 instruction received from such agencies.

3. Use of the above markings does not mean that the information cannot be released to the public under FOIA, 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. INDENTIFICATION MARKINGS:

   a. An unclassified document containing FOUO information will be marked "UNCLASSIFIED // FOR OFFICIAL USE ONLY" in bold letters at least 3/16 of an inch at the top and bottom of the front cover (if any), on the first page, on each page containing FOUO information, on each page, and on the outside of the back cover (if any). No portion markings 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 of information 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 the "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent practical.

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 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 nonworking 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 nonworking 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 by fourth-class mail. Electronic transmission of FOUO information by voice, data, facsimile 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 direct 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.

W911W4-13-R-0005-0004

US ARMY SAP ADDENDUM TO DD FORM 254

XXX (1) This contract requires access to Special Access Program (SAP). The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel, and information security for safeguarding SAPI, and are part of the security classification specification for this contract:

XXX DoD 5220.22-M-1, NISPOM, with DoD overprint and NISPOMSUB
XXX Signals Intelligence Security Regulations (SISR) (Available from the CM)
Imagery Policy Series (Available from the CM)
_____JAFAN 6/3, Protecting Special Access Program information within Information Systems
XXX JAFAN 6/9, Physical Security Standards for Special Access Program Facilities, w/ change 2
_____AR 25-2, Information Assurance
XXX AR 380-28, DA Special Security System
XXX AR 380-381, Special Access Programs (SAPS).
_____Other

_____ (2) Contract estimated completion date: TBD by prime contract

XXX (3) The name, telephone number, email address and mailing address of the Contract Monitor (CM) for the SAP portion of this contract is: **John Doe**, Government Special Access Program Security Officer (GSSO), **703-xxx-xxxx**. NIPR johndoe@us.army.mil / SIPR johndoe@mi.army.smil.mil: (The Contract Monitor and the contractor security officer must be registered in the Army Contractor Automated Verification System (ACAVS) in order to process SAP actions)

XXX (4) All DD Forms 254 prepared for subcontracts involving access to SAP under this contract must be forwarded to the GSSO for approval and then to SAPCO, G2, Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

_____(5) The contractor will submit the request for SAP visit certifications through the PSM for approval of the visit. The certification request must arrive at the PSM at least ten (10) working days prior to the visit. Visit certification requests will be processed through ACAVS.

XXX (6) The contractor will not reproduce any SAPI related material without prior written permission of the CM.

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

____ (8) Electronic processing of SAP requires accreditation of the equipment in accordance with JAFAN 6/3 and AR 25-2 (Note: Check only if item 11l indicates that a requirement exists for SAP AIS processing.)

W911W4-13-R-0005-0004

_____ (9) This contract requires a contractor SAPF.

XXX (10) This contract requires indoctrination to Special Access Program.

_____(11) The contractor will perform SAPI work under this contract at the following locations:

CERTIFICATION AND SIGNATURE, " Security requirements stated herein are completed and adequate for safeguarding the classified information released or generated under the classified effort. All questions shall be referred to the official named below".

_____ _____

Name: Date Approved

Government Special Access Program Security Officer (GSSO)