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: August 31, 2025

The public reporting burden for this collection of information, 0704-0567, is estimated to average 36 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See Instructions)*

Top Secret

b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY

None (See instructions)

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

☒ **a. PRIME CONTRACT NUMBER** *(See instructions.)*
[ADD FULL CONTRACT NUMBER/TASK ORDER]

☐ **b. SUBCONTRACT NUMBER**
SEE ITEM 13 [ADD UNCLAS OR CUI IN HEADER]

☐ **c. SOLICITATION OR OTHER NUMBER** **DUE DATE** *(YYYYMMDD)*
[ADD FCL LEVEL IN ITEM 1]

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)*
[ADD REV# + ORIGINAL DATE]

☐ **c. FINAL** *(Complete Item 5 in all cases.)* **DATE** *(YYYYMMDD)*
[ADD SAFEGUARD LEVEL IN 1b]

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)*
[ADD THE FULL/COMPLETE NAME OF COMPANY/ VENDOR AND ADDRESS] [ADD CAGE CODE TO ITEM 8b)	[CAGE]	Defense Counterintelligence & Security Agency (DCSA) [ADD NAME OF DCSA FIELD OFFICE] Field Office [ADD DCSA FIELD OFFICE IDENTIFIER] [ADD DCSA FIELD OFFICE ADDRESS] [ADD DCSA FIELD OFFICE PHONE/E-MAIL]

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)*
SEE ITEM 13		

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)*
HQ USSOCOM/[ADD DIRECTORATE/OFFICE] 7701 Tampa Point Blvd MacDill AFB, FL 33621	N/A	HQ USSOCOM/SOCS-Z-SM 7701 Tampa Point Blvd MacDill AFB, FL 33621 813-826-4333 IndustrialSecurity@socom.mil
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)*
[ADD THE FULL NAME OF GOVERNMENT AGENCY & OFFICE SYMBOL] [FULL ADDRESS & ZIP CODE [GOVERNMENT POC NAME] [GOVERNMENT POC PHONE AND E-MAIL]	N/A	[ADD NAME/OFFICE SYMBOL OF GOVERNMENT AGENCY COGNIZANT SECURITY OFFICE (CSO)] [ADD GOVERNMENT AGENCY CSO ADDRESS] [ADD GOVERNMENT AGENCY PHONE NUMBER] [ADD GOVERNMENT AGENCY E-MAIL]

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)*
[ADD THE FULL/COMPLETE NAME OF COMPANY/ VENDOR AND ADDRESS] [ADD CAGE CODE TO ITEM 8b) [ADD LEVEL OF SAFEGUARDING IN ITEM 1b]	[CAGE]	Defense Counterintelligence & Security Agency (DCSA) [ADD NAME OF DCSA FIELD OFFICE] Field Office [ADD DCSA FIELD OFFICE IDENTIFIER] [ADD DCSA FIELD OFFICE ADDRESS] [ADD DCSA FIELD OFFICE PHONE/E-MAIL]
a. LOCATION(S) *(For actual performance, see instructions.)* N/A	**b. CAGE CODE** *(If applicable, see Instructions.)*	**c. COGNIZANT SECURITY OFFICE(S) (CSO)** *(Name, Address, ZIP Code, Telephone required; Email Address optional)*

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT

[ADD UNCLASSIFIED DESCRIPTION OF THE EFFORT - TYPICALLY SAME AS PWS/SOW/IWP TITLE]

PERIOD OF PERFORMANCE: DD MMM YYYY - DD MMM YYYY (BIENNIAL DD FORM 254 REVIEW REQUIRED - SEE ITEM 13)

Controlled by: HQ USSOCOM
Controlled by: J6-ITMO
CUI Category: OPSEC
Distribution/Dissemination Control: DISTRO C
POC: Mr. Chad Morgan, 813-826-7063/DSN 299-7063, chad.morgan@socom.mil

****
THIS DD FORM 254 IS TENTATIVELY APPROVED. Upon (company selection, identification of a Contract Number/Task Order) but prior to award and any classified release, this DD Form 254 with all pertinent information inserted in appropriate sections will be submitted to U.S. Special Operations Command Industrial Security for final review and approval.
****

****
THIS DD FORM 254 IS TENTATIVELY APPROVED PENDING FACILITY CLEARANCE (FCL). Upon Defense Counterintelligence & Security Agency approval of FCL, but prior to award and any classified release, this DD Form 254 will be submitted to U.S. Special Operations Command Industrial Security for final review and approval.
****

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 GOVERNMENT INFORMATION**
- ☒ **i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION**
- ☒ **j. CONTROLLED UNCLASSIFIED INFORMATION (CUI)** *(See instructions.)*
- ☒ **k. OTHER** *(Specify)* *(See instructions.)*

SEE ITEM 13

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.)*

SEE ITEM 13

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)*

SEE ITEM 13

Public Release Authority:

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 Contracting Officer's Representative/Program Manager will provide a copy of all applicable security directives for this contract. Appropriate applicable HQ USSOCOM security directives, regulations, and standard operating procedures will be provided by the requiring agency (normally through the Performance Monitor or Component/Theater Special Operations Command COR/PM). Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified information (furnished or generated) to the source from which received unless retention or other disposition instructions are authorized in writing by the USSOCOM Government Contracting Agency/Activity. Furthermore, the contractor will account for and return all Common Access Cards (CACs) to Contracting Officer's Representative, Program Manager, or Trusted Agent upon completion or termination of the classified contract, termination of employment, or suspension of classified clearance or access of any contractor employee. Security badges, installation entry passes/vehicle decals issued to contractor personnel will be returned to the appropriate issuing office as required.

Ref 2b: IAW NISPOM, Section §117.17, subcontracting/flow-down of this effort requires a Subcontract/Flow-Down DD FM 254. Subcontract/Flow-Down DD FM 254 must be approved by HQ USSOCOM prior to award. Forward requests and draft Subcontract DD FM 254s to the Contracting Officer's Representative/Program Manager and USSOCOM Industrial Security (IndustrialSecurity@socom.mil). IAW USSOCOM R 380-9, Industrial Security, please allow 10 duty days for review/approval.

Ref 2b. Subcontractors with performance at HQ USSOCOM. IAW NISPOM, Section §117.16(a), Prime Contractor will forward subcontractor Visit Requests to HQ USSOCOM Personnel Security (PERSEC) via DISS SMO Code MA3DF8X94. Visit Requests must not be submitted to HQ USSOCOM until the Subcontract DD FM 254 is approved. Failure to follow this guidance will result in the cancellation of the Visit Request.

Ref 4: Classified material received or generated under H92404-21-D-0001, TO# H92415-25-F-E025 (Preceding Contract Number) is transferred to this follow-on contract.

Ref 7: See guidance in Ref 2b.

Ref 10a: The contractor requires administrative access to classified Communications (COMSEC) material. The contractor will not copy, or

generate classified COMSEC material. Access to classified COMSEC information requires final U.S. Government clearance at the appropriate level. Further disclosure of COMSEC information by a contractor, to include subcontracting, requires prior approval of the GCA. Non-accountable COMSEC information, though not tracked in the COMSEC material control system, may still require a level of control within a document control system. Refer to NSA/CSS Manual 3-16, Subject: Control of Communications Security Material; the Committee on National Security Systems Instruction (CNSSI) No 4001, Subject: Controlled Cryptographic Items; and the Committee on National Security Systems CNSSI No 4005, Subject: Safeguarding Communications Security Facilities and Material, for guidance. Access will be at a Government installation and will be granted by the user agency. Contractor personnel with access to classified COMSEC will follow the security requirements of the host government activity.

Ref 10b: The contractor is permitted access to Restricted Data (RD) in the performance of this contract. Access to RD requires a final U.S. Government clearance at the appropriate level.

Ref 10c: Contractor is permitted access to Critical Nuclear Weapons Design Information (CNWDI) in performance of this contract. Access to CNWDI requires a final U.S. Government clearance at the appropriate level. The government program manager or designated representative will ensure the contractor security supervisor is briefed for CNWDI. GCA approval is required prior to granting CNWDI access to a subcontractor.

Ref 10d: The contractor is permitted access to Formerly Restricted Data (FRD) in the performance of this contract. Access to FRD requires a final U.S. Government clearance at the appropriate level.

Ref 10e(1): See SCI Addendum.

Ref 10e(2): For non-SCI material, authorization and briefing shall be in accordance with the NISPOM and/or other appropriate directives. In any case, Contractor shall brief the employee or Contractor's Security Officer on the employee's obligation to safeguard the information, and the employee shall be debriefed according to the applicable regulations, when the access is terminated. When the Contractor briefs or debriefs an employee, the Contractor shall execute a separate SF Form 312, "Classified Information Nondisclosure Agreement" or another form, if required by the applicable regulation covering the material for each cleared employee who shall be afforded access to the classified/intelligence material. In each case, the form shall be appropriately annotated to indicate that a special briefing relative to safeguarding material provided to the contractor.

Ref 10f: See SAP Addendum. IAW "Implementation Guidance for DoD Special Access Program Enterprise (11 July 2023); Attachment 5 "SAP Enterprise Reform Directed Actions" (page 13), all Performance Work Statements, Statements of Objectives, Statements of Work; as well as associated DD FM 254s with a documented Special Access Program (SAP) access requirement will be marked as CUI. The required CUI Designation Indicator will include the following. The Indicator will be included at the bottom of the first page for PWSs/ SOOs/SOWs and in Item 9 on DD254s below the Period of Performance.

Controlled by: HQ USSOCOM
Controlled by: [Name of COR's Directorate/Special Staff/Division/Branch/Office]
CUI Category: OPSEC
Distribution/Dissemination Control: DISTRO C
POC: Mr. Chad Morgan, 813-826-7063/DSN 299-7063, chad.morgan@socom.mil

Ref 10g. The contractor is permitted access to North Atlantic Treaty Organization (NATO) information in performance of this contract. Access to NATO information requires a final U.S. Government clearance at the appropriate level. 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 with regards to NATO information IAW NISPOM Section §117.19, Paragraph (g). Prior approval from the contracting activity is required for subcontracting and in accordance with NISPOM Section §117.19, Paragraph (g)(9).

Ref 10h. The contractor is permitted access to Foreign Government Information (FGI) in the performance of this contract. Access to Foreign Government Information requires a final U.S. Government clearance at the appropriate level. Contractor employees will be briefed, and acknowledge in writing, their responsibilities for handling Foreign Government Information prior to being granted access. The contractor will maintain strict compliance with NISPOM, Section §117.19, Paragraph (c). Prior approval of the contracting activity is required for subcontracting and in accordance with NISPOM, Section §117.17, Paragraph a(3)(iv).

Ref 10i. Alternative Compensatory Control Measures (ACCM) Program information is governed by DoD M 5200.01-V3, DoD Information Security Program: Protection of Classified Information, Enclosure 2, Section 18; CJCS Manual 3213.02D, Joint Staff Alternative Compensatory Control Measures Program Management Manual, and supporting documentation for each ACCM sub-system, including security classification guides, program security plans, and governing directives. Inspections of ACCM information in USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), or Theater Special Operation Command (SOCNORTH, SOCAFRICA,

SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, or SOCKOR) owned and operated facilities are under the auspices of the respective Command or Component ACCM Coordinator/ACCM Program Control Officer (ACCM Coord/ACCM PCO). If applicable, ACCM material maintained by the Contractor within their facility must be afforded protection commensurate with DOD requirements and strictly controlled based on need-to-know and required briefings. DCSA personnel conducting inspections of the Contractor must be briefed on to the specific program by the appropriate government ACCM Coord/ACCM PCO responsible for the material prior to being granted access.

Ref 10j: Controlled Unclassified Information (CUI) provided under this contract shall be safeguarded as specified in the CUI Addendum included with this specification.

Ref 10k: NIPRNET/SIPRNET/JIANT/BICES/CENTRIX/JWICS/SAPNET/JIANT/CCS access required at government facilities only.

Ref 10k. Contractor will reference Defense Information Security Agency (DISA) Cloud Computing Security Requirements Guide when utilizing CCS for Information Impact Levels (ILs) and associated security requirements.

Ref 10k. Contractor requires access to Commercial Solutions for Classified (CSfC) Mobile Devices for use outside of cleared contractor facilities. As authorized by USDI & DOD CIO Memo, Security and Operational Guidance for Classified Portable Electronic Devices, dated 25 Sep 2015, select cleared and trained contractors are approved to use Commercial Solutions for Classified (CSfC) Mobile Devices in order to effectively accomplish mission requirements outside of secure government and/or cleared contractor facilities. In coordination with and through the responsible Contracting Officer's Representative/Program Manager (COR/PM), contractors will submit a USSOCOM IMT 33, CSfC Device User Agreement & Hand Receipt and an Authorization of Issuance Memorandum to their local Industrial Security Office. Authorization of Issuance Memorandums must be endorsed at the 0-6 or GS/GM-15 level at a minimum. HQ USSOCOM users will follow guidance as outlined in USSOCOM Manual 380-19, Mobility and Wireless Communications. Defense Counterintelligence and Security Agency (DCSA) is relieved of security oversight for contractors issued CSfC devices. Security oversight for contractors issued these devices falls under the purview of the issuing Government Industrial Security Office. USSOCOM issued devices will not be introduced into cleared contractor facilities or be connected to SIPRNet other than through the USSOCOM network.

Ref 11a: Contractor performance is restricted to SOCOM HQ MacDill AFB, FL, HQ USASOC, Ft Bragg, NC and NSWC, San Diego CA. Government agency or activity will provide security classification guidance for performance of this contract. Submit visit request to COR and/or Security Management Office for need-to-know verification.

Ref 11l: Controlled Unclassified Information (CUI) provided under this contract shall be safeguarded as specified in the CUI Addendum included with this specification.

Ref 11m: Access to all USSOCOM facilities requires contractors to possess a minimum of a SECRET clearance.

Ref 11m: Contractor is authorized to courier classified information up to the TOP SECRET/SCI level in performance of official duties upon approval of and designation by the COR, PM, SSO and/or Security Manager.

Ref 12: Requests must be forwarded through the responsible Contracting Officer's Representative/Program Manager, Contracting Official (Item 16) and the HQ USSOCOM Special Operations Communication Office (SOCS-SOCO), Public.Affairs@socom.mil, (813) 826-4600, prior to public release.

SCI ADDENDUM
(09 JANUARY 2026)

This supplement applies to:

Prime Contract Number: XXX
Delivery/Task Order Number: XXX

Subcontract Number: N/A
Expiration Date: XXX

The following controls will apply to Sensitive Compartmented Information (SCI) provided under this contract.

1. Item 10e (2): Security clearances for contractors working within SCIF spaces must be adjudicated meeting Intelligence Community Policy Guidance (ICPG) 704.1, 704.2, 704.3, 704.4, 704.5 eligibility requirements. Prior approval of the contracting activity is required for sub-contracting. Access to intelligence information requires special briefings and a final U.S. Government clearance at the appropriate level.

2. Item 13: Department of Defense (DOD) Manual 5105.21, Volumes 1-3, Intelligence Community Policy Guidance (ICPG) 704.1, 704.2,

704.3, 704.4, 704.5, Intelligence Community Standard (ICS) 705-1&2 including the Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities (IC Tech Spec-for ICD/ICS 705, and Headquarters, United States Special Operations Command (HQ USSOCOM) 380-6, provide the necessary guidance for physical and information security measures and are part of the SCI security specifications for the contract.

3. Item 13: Inquiries pertaining to classification guidance will be directed to the responsible USSOCOM Contracting Officer's Representative/Program Manager/Contract Monitor (Mr. Chad Morgan, (813) 826-7063).

4. Item 13: All SCI furnished to the contractor in support of this contract / delivery / task order remains the property of the DOD or the agency or command that releases the information. Upon termination of the contract, all furnished SCI will be returned to the HQ USSOCOM Special Security Office (SSO) or the prime contractor.

5. Item 14: This contract / delivery / task order requires that NUMBER (X) contract billet be established in order to fulfill the contractual obligations incurred. Access will be granted by the government agency. Upon completion or cancellation of the contract, the Contractor SSO (CSSO) will debrief or notify the HQ USSOCOM SSO to debrief all personnel not required for contract closeout and those billets will be disestablished.

6. Item 14: Names of contractor personnel requiring access to SCI and justification for SCI billets will be submitted to HQ USSOCOM SSO after contract monitor coordination. Billet justifications will include the contract statement of work. If a Tier 5 (T5) or equivalent Investigation has not been completed upon approval of billets by the HQ USSOCOM SSO, the CSSO will submit necessary forms to the Adjudication and Vetting Services (AVS) for a T5 investigation and subsequent ICD 704 – SCI Adjudicative determination. A T5, SCI Eligibility and access to SCI will comply with the National Industrial Security Program Operating Manual. Upon completion of the T5 investigation, a nomination for SCI access will be submitted to HQ USSOCOM SSO.

7. Item 14: The CSSO will advise HQ USSOCOM SSO, through the contract monitor, upon reassignment of personnel to other duties not associated with this contract. The Contract Monitor will also notify the SSO Office at SOCOM.SSO.PERSEC@SOCOM.MIL or 813-826-1287 so the SSO can remove their ownership of the contractor in DISS.

8. Item 14: The CSSO must coordinate with the SCI contract monitor before subcontracting any portion of SCI efforts involved in the contract. A separate DD Form 254 for the subcontractor will be processed and a copy provided to HQ USSOCOM SSO.

9. Item 14: The contractor will not use references to SCI access, even by unclassified acronyms, in advertisements, promotional efforts, or recruitment of employees.

10. Item 14: All SCI work will be performed at the locations specified below and in subsequent Task Orders. Prior to USSOCOM SCI level work, to include the introduction of equipment or materials, commencing under this contract at any SCIF that does not hold a "SO-" prefix in its ID, in accordance with DoDM5105.21v2 and IC-Series 705 an appropriate Co-Use or Joint-Use Agreement between the host and tenant elements must be in place and accepted by the respective accrediting authorities.

a. HQ USSOCOM, MacDill AFB FL

11. Item 15: HQ USSOCOM SSO has exclusive security responsibility for all SCI released to the contractor or developed under this contract. Defense Intelligence Agency and HQ USSOCOM SSO retain authority for all inspections of the contractor to ensure compliance with SCI directives, regulations, and instructions.

12. All contractor personnel requiring access to Sensitive Compartmented Information (SCI) under this contract must be enrolled in and maintain favorable eligibility through the government's Continuous Vetting (CV) program. This is in accordance with the Trusted Workforce 2.0 initiative. The contractor is responsible for ensuring all personnel comply with CV reporting requirements.

13. In accordance with DODM 5105.21 Volume 1-3, the following activity is designated User Agency Special Security Office for SCI requirement:

HQ USSOCOM
Special Security Office (SSO)
7701 Tampa Point Boulevard Telephone: DSN 299-1287 SOCOM.SSO.INDUSEC@SOCOM.MIL
MacDill AFB, Florida 33621-5323 Commercial: (813) 826-1287

PROTECTING SPECIAL ACCESS PROGRAM (SAP) INFORMATION
ADDENDUM
(Version 1, 29 May 2024)

Special Access Program (SAP) discussion, storage, and processing associated with this effort will be conducted in SAP Facilities (SAPF) specifically approved, in writing, by the USSOCOM SAP Management Office (SAPMO) or designated USSOCOM Program Security Officer (PSO). Contact the SAP approval official in Block 13 for approved SAPF locations.

SAP activities are governed by 32 Code of Federal Regulation Part 117, "NISPOM rule"; DoD Manual 5200.01 (DoD Information Security Program) Volumes 1-4; DoD Directive 5205.07 (Special Access Program Policy); DoD Manual 5205.07 (DoD Special Access Program Security Manual), Volumes 1-4; DoD Instruction 5205.11, (Joint SAP Implementation Guide (JSIG);
USSOCOM Manual 380-2 (SAP Security Guide); USSOCOM Manual 380-7 (USSOCOM Arms Control Readiness Inspection Program); and applicable program security classification guides and subsequent versions.

Access to SAP information requires employees to undergo additional personnel security screening and meet the requirements of DoD SAP accessing directives and policies in accordance with DoDM 5205.07, Volume 2. The individual must meet applicable eligibility requirements and possess a final Secret or Top Secret security clearance depending on the level of access required in performance of this contract. Program Access Requests (PAR) for contractor personnel must be submitted by the Contractor Program Security Officer (CPSO) to the PSO for approval by the designated Access Approval Authority (AAA). Personnel approved for access will receive a program indoctrination briefing and must sign an SAP Indoctrination Agreement (PIA) prior to receiving access to program information or material. The CPSO will maintain the signed PIA and forward a copy to the PSO for entry into the appropriate database system.

The July 20, 2023, OSD Memorandum relieves the Defense Counterintelligence and Security Agency (DCSA) from industrial security oversight of cleared defense contractors performing on contracts that require DoD SAP access. SAP inspections and security oversight of USSOCOM or Component government or contractor SAP facilities are under the cognizance of the USSOCOM PSO or SAPMO representative, as appropriate. Additional Component SAP security requirements may apply for activities conducted at Service Component or Sub-unified command locations. The Performance Monitor or component command Contracting Officer Representative (COR) at these locations/facilities will provide specific or additional guidance.

OPSEC-sensitive or classified communication will be conducted via PSO-approved secure channels from within the SAPF. Transmission of documents via secure facsimile between terminals within SAPFs may be approved by the PSO. Only the U.S. Postal Service Registered or Certified mail, if authorized, will be used to mail program material unless an alternate method is approved by the PSO. Consult the PSO prior to mailing any SAP information. Briefed personnel are authorized to courier classified information within the continental United States with written approval from the CPSO or PSO. Two (program briefed) personnel are required to courier Top Secret material unless prior approval is obtained from the PSO. Couriers will be in the possession of PSO-issued courier authorization letters prior to travel. All material, to be mailed or carried, will be wrapped, and transmitted in accordance with DoDM 5205.07, Volume 1. An inventory of material to be couriered will be provided to the PSO prior to departure of the courier(s).

Prior to processing SAP information on any Automated Information System (AJS), the contractor will provide the PSO with a System Security Plan (SSP) and other documentation required in JSIG for Assessment & Authorization (A&A) from the Authorizing Official (AO), or subsequent policy. The PSO will issue program specific Security Authorization following verification of the A&A process. USSOCOM Special Access Program (SAP) Policy Memorandum: Removable Media and Two-Person Integrity Control Policy is applicable for this contract. All requirements of USSOCOM Manual 380-3 (Cybersecurity) and 380-19 (Mobility and Wireless Communications) will be adhered to.

Reproduction of program material will be conducted only be program indoctrinated personnel using only reproduction equipment and security procedures approved by the GPSO. A single person may reproduce non-accountable (Secret and below) classified material. All Top Secret (SAP) material must be reproduced by two program-indoctrinated individuals and must be documented and brought under formal accountability procedures.

Destruction of program material will be conducted only by program indoctrinated personnel. Destruction equipment and procedures approved by the PSO. A single person may destroy non- accountable classified material. Accountable material must be destroyed and documented by two program cleared individuals.

The government PSO will be advised within 24 hours of any matters which affect the baseline facility clearance. The CPSO will also report any incident that may have an adverse impact on a personnel security clearance eligibility or access within 24 hours.

All personnel with a security clearance are required to report any information that could have an impact on their ability to protect classified information and/or as documented in Security Executive Agent Directive Three (SEAD 3) (Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position). CPSOs are reminded of their responsibilities to diligently report any significant action or any change in an employee's eligibility to the PSO immediately.

A security incident is a broad term to describe security infractions, violations, and compromises. These terms have succinct meanings; are

further explained, defined, and require specific actions by the CPSO. The DoD definitions for these terms are defined in DoD Manual 5200.01-V3. If work under this contract is authorized in contractor-controlled or operated workspaces, CPSOs are required to contact the PSO or USSOCOM SAPMO whenever a security incident occurs in the contractor-controlled workspace involving a contract employee under this effort.

Per DoD Manual 5205.07 Volume 1, Encl 11. Sec 3: "Any (contractual) relationship with a prospective subcontractor requires prior approval by the PSO." All security requirements levied upon the prime contractor will "flow-down" to the subcontractor. SAP access and other requirements must be pre-coordinated and approved by the PSO prior to staffing and implementation. All new SAP DD Form 254s for acknowledged SOF SAPs shall be marked Controlled Unclassified Information (CUI) unless the contractor relationship is approved as a sensitive industrial relationship. Then the DD 254 will be marked at a higher level. All new DD254 for unacknowledged SOF SAPs may be marked CUI or a higher classification when required. All cleared defense contractors with contracts that require access to SOF SAPs must be registered in the USSOCOM Central Repository and utilize the National Industrial Security Program Classification System unless a sensitive industrial relationship is approved.

PROTECTING “CONTROLLED UNCLASSIFIED INFORMATION” (CUI)
CUI ADDENDUM
(Updated March 2021)

1. GENERAL:

a. Controlled Unclassified Information (CUI) is not a security classification, but designates unclassified information that requires any safeguarding or dissemination control per DoD Instruction 5200.48, “Controlled Unclassified Information” (6 March 2020).

b. With the implementation of DoDI 5200.48, DoDM 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information” (24 February 2012, as amended), has been cancelled and “For Official Use Only” (FOUO) and is no longer authorized. All new documents shall be marked in accordance with the guidance below.

c. In order to balance the need to safeguard CUI with the public interest the CUI Registry, established by DoDI 5200.48, lists categories of CUI Basic/Specified and identifies basis for controls, and includes guidance on handling procedures.

d. There are two subsets of CUI.

i. CUI Basic is the subset of CUI for which law, regulation, or government policy does not set out specific handling or dissemination controls. CUI Basic handling and dissemination controls are the same as previously used for FOUO.

ii. CUI Specified is the subset of CUI for which law, regulation, or government policy contains specific handling controls that differ from CUI Basic. The government will provide marking and handling guidance separately for CUI Specified.

e. Remarking legacy FOUO documents is not required as long as they remain under DoD control. When needed, FOUO information does not automatically become CUI, so the material must be reviewed by the information owner to determine if it meets the CUI requirements and marked appropriately.

f. When responding to FOIA requests, the responsible DoD agency must base its decision on the content of the information and applicability of any of the FOIA statutory exemptions regardless of whether an agency designates or marks the information as CUI.

2. DESIGNATION as CUI: Designating CUI occurs when an authorized holder, consistent with DoDI 5200.48 and the CUI Registry, determines that a specific item of information falls into a CUI category or subcategory. The information must be designated as either CUI Basic or CUI Specified and the authorized holder must ensure that appropriate markings are applied to documents to ensure recipients are aware of the CUI status. See the associated Security Classification Guide (SCG) or other guidance provided by the Government Contracting Agency (GCA) for specific categories of CUI related to this contract and guidance on storage, handling, and dissemination.
3. MARKING:

a. Unclassified documents containing CUI will be marked CUI at the top & bottom of each page. As a best practice each “portion” (i.e. titles, subject lines, paragraphs, bullets, charts, etc.) containing CUI may be Portion Marked (CUI). If portion marks are used then Unclassified portions will be Portion Marked (U). Do not use (U//CUI).

b. The government will provide marking, handling, and dissemination guidance separately for any CUI Specified information. For classified contracts, this guidance will be contained in the associated SCG.

c. The following CUI Designation Indicator information will be included on the first/title page or cover of all unclassified documents containing CUI:

Controlled by: [Name of DoD Component and Office]
CUI Category: [List of Category or Categories of CUI]
Distribution/Dissemination Control: [Use "None" for CUI Basic/As required for CUI Specified)
POC: [Phone Number and/or E-mail]

d. Classified documents containing CUI will NOT include CUI in the banner marking at the top and bottom of each page. Each paragraph that contains only CUI will be portion marked (CUI). All other paragraphs will be marked according to their classification. Do not "co-mingle" CUI with classified information. The above CUI Designation Indicator information must be included on the first page or cover (same as unclassified documents). Additionally, the following statement must be included on the first page of documents that contain both CUI and classified information:

This content is classified at the [insert highest classification level of the document] level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer to [cite specific reference or applicable Security Classification Guide]. It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release.

4. PROCESSING: Unclassified Automated Information Systems (AIS) used to process CUI under this contract must meet the basic security requirements listed in the NIST SP 800-171 REV 2, "Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations", 21 February 2020. AIS accredited and approved for processing classified information under this contract are also approved to process DoD CUI.

5. DISSEMINATION: CUI may be disseminated between officials of DoD Agencies, DoD contractors, consultants and grantees to conduct official business for the DoD provided the dissemination is consistent with controls imposed by a Distribution Statement or Limited Dissemination Controls (LDC). Guidance on Distribution Statements and LDCs will be provided separately by the government for any prescribed CUI Specified information. For classified contracts, this information will be contained in the program SCG. CUI always requires Foreign Disclosure Decision before release outside of DoD Agencies, DoD contractors, consultants and grantees.

6. STORAGE: During working hours, to prevent unauthorized access, do not leave CUI unattended, read or discuss around unauthorized personnel. CUI 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: CUI may be transmitted using the following:

a. Mail – CUI may be sent via first class mail or parcel post. Bulk shipments may be sent by fourth class mail. Contents must be properly marked, but no markings will appear on the outer wrapper.

b. Fax – Normally CUI may be sent via Facsimile equipment. To prevent unauthorized disclosure, coversheets should be used, the locations of both fax machines should be considered, and availability of an authorized recipient at the receiving end should be confirmed. Secure classified fax machines may be used without the above verifications.

c. E-Mail/Web Sites – E-mail may be used on approved secure communication systems or systems using other protective measures such as Public Key Infrastructure (PKI) or transport layer security (e.g., https). E-mail messages must be appropriately marked to identify CUI status. Personnel will not use unofficial or personal email accounts, messaging systems, or other non-DoD information systems, except approved government contractor systems to conduct official business involving CUI.

d. Video Teleconferencing – Only use Government Agency approved secure, encrypted video conferencing and collaborative platforms (i.e. SVTC, etc.). CUI may not be discussed over commercially available video conferencing applications.

e. Avoid wireless transmission unless no other means are available.

8. DESTRUCTION: When no longer needed, CUI must be disposed of in a way that will make it unreadable, indecipherable, and irrecoverable. Use of approved sensitive/classified material destruction devices is recommended. (ISOO CUI Notice 2019-03, "Destroying

Controlled Unclassified Information in Paper Form", 15 July 2019)

9. UNAUTHORIZED DISCLOSURE: Report misuse, mishandling, or Unauthorized Disclosure of CUI to the Unauthorized Disclosure Program Management Office, the Controlling Agency and the appropriate Military Department Counterintelligence Organization. While Unauthorized Disclosure of CUI does not constitute a security violation, a formal security inquiry/investigation is required if disciplinary action will be taken against the individual(s) responsible. Unauthorized Disclosure of certain CUI, such as export controlled-technical data, may also result in civil and criminal sanctions against responsible persons based on procedures codified in relevant law, regulation, or government-wide policy.

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
HQ USSOCOM/[ADD COR/PM DIRECTORATE/ OFFICE SYMBOL] [ADD COR/PM PHONE NUMBER/DSN/E-MAIL]	[ADD COR/PM FULL NAME] Contracting Officer's Representative	
[IF SCI ACCESS, ADD] HQ USSOCOM/J2-SSO 813-826-1287/DSN 299-1287 SOCOM.SSO.INDUSEC@socom.mil	J. TUESDAY LITTLE HQ USSOCOM SSO Industrial Security	
[IF SAP ACCESS, ADD] HQ USSOCOM/SOCS-CORB 813-826-4669/DSN 299-4669 SAPCO@socom.mil	Dr. Michael J. Wentling USSOCOM SAPMO Industrial Security	
[IF SUBCONTRACT/FLOW-DOWN, ADD] HQ USSOCOM/SOCS-Z-SM, 813-826-4333/DSN 299-4333, IndustrialSecurity@socom.mil	John T. Fredette HQ USSOCOM Industrial Security	

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.)*

While performing duties at USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), Theater Special Operation Command (SOCNORTH, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, SOCAFRICA, or SOCKOR) or other U.S. Government owned and operated facilities, the contractor will adhere to the applicable Information Security Program, ADP and DODIIS Programs, Physical Security Program, Industrial Security Program, and SCI/SAP Program (if applicable). Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a U.S. Government clearance at the appropriate level.

Training Requirement: Contractors performing on this contract at military installations are required to conduct command and unit specific security training (Initial/Refresher INFOSEC, OPSEC, EMSEC, AT/FP, Intelligence Oversight, etc.). This training will be provided by the responsible military organization.

IA requirements: Specific Information Assurance requirements may be mandated and are authorized by the responsible command/unit where primary performance location is identified.

In the event that no government employee or military service member is otherwise available, the contractor may be required to conduct security-related functions (traditionally considered inherently government functions) such as escorting cleared/un-cleared visitors, opening/ closing of security containers, conducting end-of-day security checks, and arming/de-arming alarm security systems within open/non-open Collateral storage areas and Sensitive Compartmented Information Facilities (SCIFs) used for the safeguarding of classified information/ material. In support of this, the contractor is approved to conduct the above actions for the following facilities and buildings/rooms/suites.

- MacDill AFB, USSOCOM, Bldg. 501 Rooms 1106A and 2107

In the event that the contractor fails to properly conduct these responsibilities and a security violation/incident occurs, the government will have the option to take action against the company IAW U.S. law. In addition, the company will be responsible for reviewing preliminary inquiry reports for any security violation/incident for which an employee is found culpable and provide a written response to the Government Contracting Agency (GCA) and the responsible Industrial Security Program Manager for actions taken against the employee.

All security violations/incidents will be reported to the responsible Cognizant Security Office, Facility Security Officer, Contracting Officer, and contract officer representative (COR) for the contract.

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.)*

Defense Counterintelligence and Security Agency (DCSA) is relieved of all inspection responsibility within USSOCOM, Component (JSOC, AFSOC, NSWC, MARSOC, or USASOC), Theater Special Operation Command (SOCNORTH, SOCCENT, SOCEUR, SOCPAC, SOCSOUTH, SOCAFRICA, SOCKOR) and other U.S. Government owned and operated facilities.

DCSA is relieved of inspection responsibility of contractors issued Commercial Solutions for Classified (CSfC) Mobile Devices. Security oversight for contractors issued these devices falls under the purview of the issuing Government Industrial Security Office.

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

a. GCA NAME [ADD GCA NAME]	**c. ADDRESS** *(Include ZIP Code)* [ADD FULL ADDRESS] [ADD DODAAC TO ITEM 16b) [ADD CONTRACTING OFFICER'S PHONE & EMAIL IN ITEMs 16e & 16f]	**d. POC NAME** [ADD KO NAME, PHONE & E-MAIL]
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*		**e. POC TELEPHONE** *(Include Area Code)*
		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)* FREDETTE, JOHN T.	**d. AAC OF THE CONTRACTING OFFICE** *(See Instructions)* N/A	**h. SIGNATURE**
b. TITLE Industrial Security Program Manager	**e. CAGE CODE OF THE PRIME CONTRACTOR** *(See Instructions.)* N/A	
c. ADDRESS *(Include ZIP Code)* HQ USSOCOM/SOCS-Z-SM 7701 Tampa Point Blvd MacDill AFB, FL 33621	**f. TELEPHONE** *(Include Area Code)* +1 (813) 826-4333	**i. DATE SIGNED** *(See Instructions)*
	g. EMAIL ADDRESS *(See Instructions)* john.fredette@socom.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.)*

[UPDATE THE FOLLOWING AS NECESSARY]
HQ USSOCOM SMO/SSO/SAPCO