

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

(The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)

OMB No. 0704-0567
OMB approval expires:
May 31, 2022

The public reporting burden for this collection of information, 0704-0567, is estimated to average 70 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)

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

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

- ☒ **a. PRIME CONTRACT NUMBER** (See instructions.)
- ☐ **b. SUBCONTRACT NUMBER**
- ☐ **c. SOLICITATION OR OTHER NUMBER** DUE DATE (YYYYMMDD)

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

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

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

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

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

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

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

a. NAME, ADDRESS, AND ZIP CODE

b. CAGE CODE

c. COGNIZANT SECURITY OFFICE(S) (CSO)
(Name, Address, ZIP Code, Telephone required; Email Address optional)

7. SUBCONTRACTOR(S) (Click button if you choose to add or list the subcontractors
-- but will still require a separate DD Form 254 issued by a prime contractor to each subcontractor)

a. NAME, ADDRESS, AND ZIP CODE

b. CAGE CODE

c. COGNIZANT SECURITY OFFICE(S) (CSO)
(Name, Address, ZIP Code, Telephone required; Email Address optional)

8. ACTUAL PERFORMANCE (Click button to add more locations.)

a. LOCATION(S) (For actual performance, see instructions.)
HQ US CENTRAL COMMAND
7115 S. Boundary Blvd.
MacDill AFB, FL 3362-5101

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

USCENTCOM requires services (non-personal) to support a unique joint staff planning need focused on integrating and synchronizing Department of Defense (DoD) military activities with United States Government (USG) strategy. Services include developing draft inputs to strategies, campaign plans, and concepts of operation that ultimately translate strategic and operational objectives into a series of related activities and operations to achieve desired end states in coordination with other DoD components, USG agencies, allied, and regional partners.

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 instructions)

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

- ☒ a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY
(Applicable only if there is no access or storage required at contractor facility. See instructions.)
- ☐ b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY
- ☐ c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL
- ☐ d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE
- ☐ e. PERFORM SERVICES ONLY
- ☒ f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES
- ☐ g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER
- ☐ h. REQUIRE A COMSEC ACCOUNT
- ☐ i. HAVE A TEMPEST REQUIREMENT
- ☐ j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS
- ☐ k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE
- ☒ l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI).
(DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)
- ☒ m. OTHER (Specify) (See instructions.)
(See instructions)

12. PUBLIC RELEASE

Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual (NISPOM) or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified here with at least office and phone contact information and if available, an e-mail address. (See instructions)

☐ DIRECT

☒ THROUGH (Specify below)

US Central Command Public Affairs Office
7115 S. Boundary Blvd. MacDill AFB, FL 3362-5101

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.)

Section 12: Disclosure of any information related to this contract (classified or unclassified) is strictly prohibited without the expressed written consent of the CO/COR. This includes, but is not limited to, use or information in unclassified brochures, promotion sales, literature, reports to stockholders, or similar material.

Item 10a. Contractor must forward request for COMSEC material/information through the Contracting Officers Representative (COR). The contractor is governed by DoD 5220.22-M, Chapter 9, Section 4 "Communications Security (COMSEC)" and NSA/CSS Policy Manual 3-16. Access to COMSEC material is restricted to US citizens holding a final US Government security clearance. Such information is not releasable to personnel holding only reciprocal clearance. Prior approval from the Government Contracting Agency is required in order for a Prime Contractor to grant COMSEC access to a Subcontractor. Contractor must comply with USCENTCOM guidelines. The NSA Central Office of Record has primary responsibility for the auditing of all COMSEC material governed by DoD 5220.22-M.

Item 10b. Access to Restricted Data requires a final U.S. Government Secret or Top Secret clearance, depending upon material to be

accessed. Contractor must follow the guidelines as outlined in DoD Instruction 5210.02 and DoD 5220.22-M.

Item 10c. Access requires a final U.S. government at the appropriate level and must be coordinated through USCENTCOM SSO. GCA approval is required prior to granting CNWDI access to subcontractor(s).

Item 10d. Access to Formerly Restricted Data requires a final U.S. government Secret or Top Secret clearance, depending upon material to be accessed. Contractor must follow the guidelines as outlined in DoD Directive 5210.02 and DoD 5220.22-M.

Item 10e. (1) See attached SCI Release of Intelligence Information for additional security requirements. Access to intelligence information requires SCI indoctrination and a Top Secret U.S. Government clearance. Contractor will require access to ICD 703 "Protection of Classified National Intelligence Including Sensitive Compartmented Information" for SCI requirements. The contract must provide individuals who are able to achieve and maintain the adjudicative standards set forth in the Intelligence Community Directive (ICD) Number 704 "Personnel Security Standards and Procedures Governing Eligibility For Access to Sensitive Compartmented Information and Other Controlled Access Program Information" for continued employment. SCI access by contractor personnel must be approved in writing by the COR via nomination letter. The COR will ensure access is granted to the minimum number of employees required on the strictest need-to-know basis.

Item 10e. (2) See attached Non-SCI Release of Intelligence Information for additional security requirements. Contractor will require access to ICD 710 "Classification and Control Markings System" (11 SEP 2009). All contractor personnel assigned under this contract must possess a current U.S. Government clearance. Personnel are required to sign a non-disclosure statement. USCENTCOM SSO will provide personnel security guidance for the performance of this contract.

Item 10f. The USCENTCOM Special Access Program (SAP) Program Manager (or appropriate User Activity) is responsible for contractor access for USCENTCOM SAP material. Access to SAP information requires a final U.S. Government clearance at the appropriate level or as identified by the SAP Manager for each appropriate SAP. The contractor must coordinate with the SAP Program Manager, through the CO/COR, prior to access. They must adhere to the special access requirements/procedures developed by the SAP Office of Primary Responsibility. SAP information/material will be processed IAW DoDM 5205.07 (series) Volume 1-4, and affiliated Service/Agency Regulations. SAP Program Manager must approval all such accesses. If a SAP sub-contract is awarded, it is the prime contractor's responsibility to incorporate the additional security requirements in the sub-contract. Authority for access must be obtained from the USCENTCOM SAP Program Manager when the Need-to-Know is established and required to accomplish the required efforts under this contract. All SAP material remains the property of the releasing Government User Agency. Upon completion or cancellation of this contract, SAP material previously furnished will be returned to the direct custody of the appropriate Special Access Program Central Office (SAPCO), to include final reports produced at the SAP level. The SAP Program Manager will provide security classification guidance for the performance of the contract. Contractor personnel must adhere to the special access requirements/procedures developed by the SAP Program Manager.

Item 10g. Access to NATO material will be required for reference at the Government, or appropriately cleared contractor's facility. Access requires a final U.S. Government security clearance at the appropriate level. Contractor personnel who require access to NATO material will be briefed by the Government Contracting Agency. The Prime Contractor must receive approval from the Government Contracting Agency to grant NATO access to a subcontractor. Contractor personnel shall be debriefed by the Government Cognizant Agency prior to departure from this contract.

Item 10h. Prior approval from the Contracting Officer Representative is required for access to foreign government information for the performance of this contract. Foreign government information must be protected at the equivalent level provided to similar categories of U.S. government information or as specified by the Foreign Government in written government to-government agreements.

Item 10i. Alternative Compensatory Control Measures (ACCM): During the course of the execution of duties while assigned to USCENTCOM, individuals assigned to this contract may require access onsite to ACCM information as determined by the COR and local ACCM control officer. Individuals shall handle the information in accordance with DoDM 5200.01(series), Volumes 1-4; CJCSM 3213.02(series) and applicable program security plans and security classification guidance.

Item 10j. Controlled Unclassified Information (CUI): The contractor is authorized and may have access to UNCLASSIFIED information/material identified as "For Official Use Only" (CUI). The contractor is prohibited from further disclosure/dissemination of this information without the expressed written authorization of USCENTCOM. FOUO information provided under this contact shall be safeguarded as specified in DoDM 5200.01, Volume 4, Incorporating Change 1, May 4, 2018 and may be supplemented by USCENTCOM. In addition, contractors or subcontractors must obtain written approval from USCENTCOM CO/COR/COTR or USCENTCOM Public Affairs prior to posting any unclassified information on any web site or the internet.

Item 10k. OTHER INFORMATION.

All unclassified DOD Information in the possession of non-DOD entities on non-DOD information systems shall be protected in accordance with DODI 8582.01.

Contractors will require access to NIPRNET, SIPRNET, JWICS at Government locations.

Item 11f. Personnel must report foreign travel to the USCENCOM SSO at least 30 days prior to projected departure date. Overseas places of performance are expected to include: Various locations throughout the CENTCOM AOR and other locations as directed by the COR.

Item 11m. All provisions of ICD (Intelligence Community Directive) 503 "Policy for Information Technology Systems Security Risk Management, Certification and Accreditation" and DOD Information Technology Security Certifications and Accreditation Process apply.

Contractors shall provide all cleared employees with security training and briefings commensurate with their involvement with classified information. The contractor shall provide all cleared employees with some form of security education and training at least annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep cleared employees informed of appropriate changes in security regulations. Contractors shall maintain records about the programs offered and employee participation in them. Contractors may obtain defensive security, threat awareness, and other education and training information and material from their CSA or other sources.

Only contractor/subcontractors/consultant personnel properly nominated by the contractor and approved by the CENTCOM SSO are authorized to perform on this contract and have access to classified information/material.

General Information:

1. A Collateral or SCI Access Request letter must be submitted to the USCENCOM SSO prior to contractor gaining access to USCENCOM facilities. Signatures are required from COR, FSO, and sub-contractor's FSO, if applicable.
2. Company or COR will notify the CENTCOM SSO, Industrial Security, 813-529-2121, of all contractors who have departed or are no longer performing on the contract.
3. The contractor must relinquish government issued credentials consisting of USCENCOM badge, common Access Card (CAC), and Courier Card, when applicable, and any other government issued badges or system access cards upon resignation, termination from contract, and termination from company, suspension or revocation of security clearance or end of period of performance of contract.
4. Departure without Debrief: The CSSO/FSO accesses JPAS to ensure contractor completed SCI debrief with the USCENCOM SSO. If JPAS reflects SCI access associated with the respective contract company's Security Management Office Code, the CSSO/FSO will contact the COR advising the contractor did not out-process through the USCENCOM SSO to initiate administrative debrief and that the CSSO/FSO will take possession of government issued credentials from contract personnel upon discontinuing contract support with USCENCOM to ensure the SSO takes immediate action to facilitate deactivation and revocation of credentials and administrative SCI debriefing within JPAS.
5. All classified visit requests by contractors shall be forwarded to the COR for approval and need-to-know certification before being sent to the facility to be visited.
6. All classified information received and/or generated under this contract is the property of the U.S. Government regardless of proprietary claims. Upon completion or termination of this contract, the U.S. Government will be contacted for destruction or disposition instructions.
7. All contract personnel providing support to the referenced contract are required to adhere to all requirements identified in the SOW/PWS, DD254, applicable Federal, DOD, and USCENCOM directives, instructions and standard operating procedures that includes proper handling and safeguarding classified and un-classified information. Sponsor rules, regulations, direction, and requirements issued by COR or other authorized personnel for good order, administration, and security will apply to all Contractor personnel who enter the Government's facilities. The Contractor shall comply with established security procedures for entering a facility and/or any special procedures that may be established for certain restricted areas. All persons granted access to premises in connection with the performance of this contract will be subject to the provisions of criminal or other laws protecting classified or intelligence information, including provisions of the espionage laws (sections 793, 794 and 798 of Title 18, USC) provisions of the Intelligence Identities Protection Act of 1982 (P.L. 97-200, 50 U.S.C.421, 601) and Section 1903 of Title 32, Code of Federal Regulations (CFR).
8. Performance under the contract may require that the Contractor access data and information sensitive to another government agency, another government contractor, or of such nature that its dissemination or use other than as specified in this contract would be adverse to the interests of the government or other. Neither the Contractor, nor its contractor employees, shall divulge or release any information

developed or obtained in the course of contract performance, except to specifically authorized Government personnel or upon written approval of the Contract Officer. The contractor shall not use, disclose or reproduce any sensitive contract information that bears a restrictive legend, other than as specified in this contract.

9. Safeguarding: Contract facility must possess and retain the safeguarding clearance level granted by the Defense Security Service that is equal to or higher identified by contract.

10. Courier Authorization: Contract personnel shall not courier classified information outside any of the locations in 8a without receiving the required training/briefings and Courier Authorization Card. Hand carrying classified material OCONUS must be approved by CENTCOM SSO.

11. Foreign Travel: Individuals anticipating official or unofficial foreign travel must notify their supervisory chain of command and submit USCENCOM SSO Foreign Travel Report NLT 30 days prior to the projected departure date. All personnel conducting travel must review the Electronic Foreign Clearance Guide for country specific guidance and training. Personnel must complete USCENCOM SSO Foreign travel and Contact Questionnaires within 72 hours of return.

12. Security Infraction/Violations: It is the responsibility of all cleared personnel to report any security incident to the appropriate SSO or local security official. In the event of a suspected or verified security violation associated with this contract or pre-award effort, the Facility Security Officer (FSO) or appropriate program security officer must notify their COR within 24-hours of their knowledge of the incident. The COR will advise USCENCOM SSO, (813) 529-2121/2126, immediately upon notification from the contractor. DoDM 5105.21-V3 and CCR 380-1.

13. The SSO must be notified within 24 hours of any lost or stolen badges.

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

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.)

Foreign nationals are prohibited from access to any classified information unless sanctioned by an international or cooperative program agreement.

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.)

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

a. GCA NAME

c. ADDRESS (Include ZIP Code)

d. POC NAME

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)

b. TITLE	d. AAC OF THE CONTRACTING OFFICE (See Instructions)	h. SIGNATURE
c. ADDRESS (Include ZIP Code)	e. CAGE CODE OF THE PRIME CONTRACTOR (See Instructions.)	
	f. TELEPHONE (Include Area Code)	i. DATE SIGNED (See Instructions)
	g. EMAIL ADDRESS (See Instructions)	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

- ☒ a. CONTRACTOR
- ☐ b. SUBCONTRACTOR
- ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- ☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- ☐ e. ADMINISTRATIVE CONTRACTING OFFICER
- ☐ f. OTHER AS NECESSARY (If more room is needed, continue in Item 13 or on additional page if necessary.)

DRAFT