

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

OMB No. 0704-0567
 OMB approval expires:
 August 31, 2028

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

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)

SECRET

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

SECRET

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)
 HQ085426RE004 20260925

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 contractors request dated , retention of the classified material is authorized for the period of: days

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)

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

Advanced Planning Services (APS) will provide Architect-Engineer services, technical support and design in support of the Missile Defense Agency (MDA) in executing the advanced planning activities required to site Next Generation Missile Defense (NGMD) architecture.

10. CONTRACTOR WILL REQUIRE ACCESS TO: (X all that apply. Provide details in Block 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.)

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: (X all that apply. Provide details in Block 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.)

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)
- MDAPressOperations@mda.mil and simultaneously provide courtesy copy to the appropriate PCO.

Public Release Authority:
Missile Defense Agency, Public Affairs Office is the public release approval 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.)

Facility Security Clearance: The Contractor shall possess and maintain a facility clearance granted by the Defense Counterintelligence and Security Agency (DCSA). The Contractor's employees, performing work in support of this contract (not technicians as stated below) will require security clearance/eligibility determination based on a favorably adjudicated T5 or T5R with SCI eligibility; be within investigation scope and/or currently enrolled in Continuous Evaluation (CE) / Continuous Vetting (CV) at the time of contract award and throughout the life of the contract to include all potential option years identified in this PWS. The DD 254 will be housed within the NCCS through the life of the contract. The Contractor shall be registered within NCCS at time of award to gain access to the DD 254. It is incumbent upon the Contractor to ensure that the necessary security paperwork is submitted in sufficient time to enable each individual to be cleared prior to beginning work on this contract. In the event that the NCCS is superseded by another System of Record, the same requirements apply. The Contracting Officer will maintain the DD254 in the Official Contracts Records.

– Contractor personnel performing or assigned under this contract must be U.S. persons. Security Classification Guide requests should be presented to the Government Sponsor, if required, subsequent to contract award. All classified information received or generated under this contract is the property of the U. S. Government. The U. S. Government shall provide disposition instructions. No release of classified information or controlled unclassified information under this contract is authorized. All requirements for control and accounting of original documentation and copies apply. All applicable provisions of the NISPOM and its supplements and 32 CFR, part 117 apply. Any classified information shall be transmitted IAW DOD 5200.1-R, DOD Information Security Program

Regulations. The contractor shall adhere to Chapter 8, NISPOM, which applies to non-DoD IT systems.

Contractor is not authorized to subcontract on this effort without an approved subcontracting plan with written GCA/COR authorization

- All Common Access Cards (CACs), building access badges, and parking passes must be returned immediately at the end of the period of performance date.
- The Contractor shall comply with (1) Security Agreement (DD Form 441/DD Form 441-1), including the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M and any revisions and (2) 32 CFR, Part 117. Provisions of the Privacy Act apply to all records and reports maintained by the contractors.
- All programs and materials developed at government expense during the performance period of this contract are the property of the US Government.
- Prior to granting an employee access to classified information and/or materials, the contractor shall brief employees with regard to their obligation to comply with the NISPOM, to include any changes and/or amendments, and 32 CFR Part 117. The contractor's employees shall be debriefed when access to the material is no longer needed or is terminated. A list of all employees who have had access to classified information during the period of this contract shall be maintained by the contractor company and be available for Defense Counterintelligence and Security Agency inspection
- Access to General Protection/Security Policies and Procedures. All contractor employees, including subcontractor employees stationed or assigned on a US Government facility shall comply with applicable installation, facility access procedures and local security policies (provided by the US Government security personnel). The contractor workforce shall comply with all personal identification verification requirements as directed by local policy. In addition to the changes otherwise authorized by the changes clause in this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the US Government may require changes in the contractor security processes or procedures.

Contractors requiring access to US Government Information Technology (IT) systems must adhere to all US Government requirements. All contractor employees and any associated subcontractor employees shall annually complete the DoD Information Assurance Training and sign an Acceptable Use Policy (AUP). The training certificate and AUP must be provided to the designated personnel at US Government facilities before issuance of network access and annually thereafter.

Contractor employees shall abide by US Government Security Regulations and Security Standard Operating Procedures when working on-site at US Government facilities/installations and shall annually attend Government mandatory training including Operational Security, Security Awareness, Subversion and Espionage, Ethics and Prevention of Sexual Harassment, and any/all other training as directed by the US Government.

Common Access Cards (CACs) are authorized for contractor employees that work on-site at Government facilities. CACs are the property of the US Government and shall be given to the Contractor Facility Security Officer upon termination of employment with the company, expiration of the CAC, replacement of a CAC, or upon contract completion. The FSO shall immediately return the CACs to the Government Security Office, Government Contracting Officer, or Contracting Officer Representative. The loss of a CAC shall be reported on the first business day following the discovery of the lost CAC to your chain of command and to the issuing agency. Unauthorized possession of a CAC can be prosecuted criminally under section 701, title 18, United States Code.

Photocopying of US Government Identification (CAC) is a violation of Title 18, US Code Part 1, Chapter 33, Section 01 and punishable by both fine and imprisonment. Although the asking for military/government identification is totally permissible by commercial establishments, there is a prohibition on duplication of government identification. A state issued driver license or other form of photo identification should be provided to be photocopied if an establishment insists on a photocopy of the traveler's identification. Contractor is required to ensure that all employees are aware of this law.

Contractor personnel shall utilize US Government or official company e-mail for transmitting official US Government business.

Official US Government business shall NOT be transmitted via personal, private, and/or commercial e-mail accounts, i.e., YAHOO, HOTMAIL, GMAIL, VERIZON etc.

Contractor is prohibited from using reference to this contract, classification, clearances, accesses (collateral and/or SCI), even by unclassified acronyms, in advertisements, websites, capabilities fliers, promotional efforts, or recruitment of employees.

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. An approved subcontracting plan and Government Contracting Officer written approval is required prior to granting Restricted Data access to a subcontractor.

Ref 10j: Controlled Unclassified Information (CUI) / Receive, Store, or Generate Controlled Unclassified Information (CUI): Contractor will be provided and will abide by DoD Regulation 5400.7, DoD Freedom of Information Act Program, and DoD 5200.01-M, Information Security Program. Guidance provided under separate cover. In accordance with DoD Instruction 5200.48 (DoDI 5200.48) dated March 6, 2020, Contractors are required to ensure all personnel receive and complete Initial and Annual Refresher CUI education and training and maintain documentation of this training for audit purposes. Initial and Annual Refresher CUI security education, training and awareness on the required topics identified in Section 2002:30 of Title 32 CFR, including protection and management of CUI, to DoD personnel and contractors through the Center for Development of Security Excellence (CDSE).

CUI Courses and Resources Created for Industry:

The Center for Development of Security Excellence (CDSE) has developed an eLearning course titled DoD Controlled Unclassified Information (CUI) Training For Contractors (IF141.06.FY21.CTR). The course fulfills CUI training requirements for industry.

Additionally, CDSE has a CUI Toolkit available at <https://www.cdse.edu/toolkits/cui/current.html>. The Toolkit includes training, policy documents, resources, and an FAQ video.

Review the DoD CUI Registry at <https://www.dodcui.mil> to become familiar with CUI organizational index groupings and CUI categories. Policy documents addressing CUI oversight:

DoDI 5200.48 "Controlled Unclassified

Information." (<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF>)

32 CFR 2002 Part IV National Archives and Records Administration 32 CFR Part 2002 Controlled Unclassified Information (<https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf>)

E.O. 13556 Vol 75, No 216. Controlled Unclassified Information

(<https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf>)

-- NIST Special Publication 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>)

Question 11c Security Guidance

Ref 111: Controlled Unclassified Information (CUI) / Receive, Store, or Generate Controlled Unclassified Information (CUI): Contractor will be provided and will abide by DoD Regulation 5400.7, DoD Freedom of Information Act Program, and DoD 5200.01-M, Information Security Program. Guidance provided under separate cover. In accordance with DoD Instruction 5200.48 (DoDI 5200.48) dated March 6, 2020, Contractors are required to ensure all personnel receive and complete Initial and Annual Refresher CUI education and training and maintain documentation of this training for audit purposes. Initial and Annual Refresher CUI security education, training and awareness on the required topics identified in Section 2002.30 of Title 32 CFR, including protection and management of CUI, to DoD personnel and contractors through the Center for Development of Security Excellence (CDSE).

- CUI Courses and Resources Created for Industry:
- The Center for Development of Security Excellence (CDSE) has developed an eLearning course title DoD Controlled Unclassified Information (CUI) Training For Contractors (IF141.06.FY21.CTR). The course fulfills CUI training requirements for industry.
- Additionally, CDSE has a CUI Toolkit available at <https://www.cdse.edu/toolkits/cui/current.html>. The Toolkit includes training, policy documents, resources, and an FAQ video.
- Review the DoD CUI Registry at <https://www.dodcui.mil> to become familiar with CUI organizational index groupings and CUI categories. Policy documents addressing CUI oversight:
 - DoDI 5200.48 "Controlled Unclassified Information." (<https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF>)
 - 32 CFR 2002 Part IV National Archives and Records Administration 32 CFR Part 002 Controlled Unclassified Information (<https://www.govinfo.gov/content/pkg/CFR-2017-title32-vol6/pdf/CFR-2017-title32-vol6-part2002.pdf>)
- E.O. 13556 Vol 75, No 216. Controlled Unclassified Information (<https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf>)
- NIST Special Publication 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (<https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final>)

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.)

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

Missile Defense Agency

c. ADDRESS (Include ZIP Code)

Building 5224, Martin Road
Redstone Arsenal, AL 35741

d. POC NAME

e. POC TELEPHONE (Include Area Code)

b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE (See Instructions)

HQ0147

f. EMAIL ADDRESS (See Instructions)

17. CERTIFICATION AND SIGNATURES

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

a. TYPED NAME OF CERTIFYING OFFICIAL (Last, First, Middle Initial) (See Instructions)	d. AAC OF THE CONTRACTING OFFICE (See Instructions) HQ0147	h. SIGNATURE
b. TITLE	e. CAGE CODE OF THE PRIME CONTRACTOR (See Instructions)	
c. ADDRESS (Include ZIP Code) Building 5222 Martin Road Redstone Arsenal, AL 35898		i. DATE SIGNED (See Instructions)
	g. EMAIL ADDRESS (See Instructions)	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

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