NATIONAL SECURITY SPACE LAUNCH (NSSL)
PHASE 3 LANE 2 LAUNCH SERVICE PROCUREMENT
FA8811-23-R-0002

ATTACHMENT 2A
DD 254
CONTRACT SECURITY CLASSIFICATION SPECIFICATIONS

dRFP #2: 13 July 2023

United States Space Force
Space Systems Command (SSC)
Assured Access to Space (AATS)
Los Angeles Space Force Base, California

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: 20220531

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
Top 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)*
FA8811-23-R-0002

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)*
TBD	TBD	TBD

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)*
N/A	N/A	N/A

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)*
TBD		TBD

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT
This document serves as a blanket DD 254 for the National Security Space Launch (NSSL) Program Phase 3 Lane 2 Procurement contract. This contract allows the United States Space Force (USSF) to procure the necessary services in order to reliably launch National Security Space (NSS) space vehicles, placing payloads into their appropriate earth orbit.

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 GOVERMENT 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. 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 Block 13 continuation page

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)*	**Public Release Authority:**
SSC/AA (Security) SSC.LE.Securityworkflow@spaceforce.mil 483 N. AVIATION BLVD, EL SEGUNDO, CA 90245	SSC/PA, SSC.PA@spaceforce.mil, 310-652-1131 483 N. AVIATION BLVD, EL SEGUNDO, CA 90245

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.)

FAR 52.204-2 Security Requirements. Security Requirements Clause: (a) This clause applies to the extent that this contract involves access to information classified up to "Top Secret"; (b) The Contractor shall comply with (1) The Security Agreement (DD Form 441/DD Form 254), including 32 Code of Federal Regulation (CFR) Part 117, National Industrial Security Program Operating Manual (NISPOM); and (2) Any revisions to that manual, notice of which has been furnished to the Contractor. (c) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract. (d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

By signing this form, the requesting Government program office and the servicing Contractor (or Subcontractor) verify that the stated access requests on this form are based on legitimate and bona fide need(s)/requirement(s) of the Government.

(U) Period of Performance: Contract Award - XXXXX.

General Security - Space Systems Command, Assured Access to Space (SSC/AA), has determined that performance of this contract requires that the contractor, subcontractor(s), vendor(s), etc. (herein known as contractor), requires access to classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility if applicable, as directed by the Defense Counterintelligence and Security Agency (DCSA).

Any firm or business under contract with the United States Space Force (USSF), which requires access to classified information, will require a facility security clearance commensurate with the level of access required. Firms that do not possess a facility clearance, or the requisite level of facility clearance, will be sponsored for a Department of Defense (DoD) facility clearance.

For access to classified information, the contractor will ensure all required actions IAW DoD Manual (DoDM) 5220.22, Vol 2, Section 5 are completed for personnel working on this contract. Interim clearances are authorized except when the contractor will require NATO and COMSEC access, where a finalized security clearance is required. Security clearances are in accordance with the NISPOM. Access to SCI will be in accordance with the current SCI Addendum and DoDM 5105.21 Volumes 1-3 for SCI management.

This is also applicable to Subcontractor and Contractor personnel who are visiting or on a temporary duty assignment at the launch site. This requirement is for personnel who have or may need access to launch site restricted or controlled areas containing (NSSL) National Security Space Launch and/or Information Systems, which directly affect a launch system. Alternate Personnel Security determinations (when applicable) must be appropriately authorized in the AFSPC 31-101 supplement and validated/approved.

Security Management - The contractor shall appoint a senior official to act as the Facility Security Officer (FSO). The individual will interface with SSC/AA Security on all security matters, to include physical, personnel, industrial, information, program protection and cybersecurity and will protect all Government information and data accessed by the Contractor.

Contractor employees who become eligible for access to classified National Security Information shall receive annual refresher training in accordance with the NISPOM. In the event classified information is inadvertently received by a contractor who does not hold an active security clearance at the appropriate level, a Government employee or Contractor with the appropriate security clearance equal to or higher than the classified information received, will take possession of the material and shall safeguard and store the information in accordance with standards set forth in the NISPOM. The inadvertent disclosure will be immediately reported to their supervisor and then to SSC/AA's Security Manager for action as appropriate.

Government Contracting Activity (GCA) may award a contract requiring access and/or storage to classified information prior to the issuance of the Facility Security Clearance (FCL), but will not grant access to classified information until DCSA grants the FCL. The prime contractor for a classified procurement must have a valid FCL at the highest level of classified information involved in the contract, even if a subcontractor will perform all classified activity. Contractors are authorized to possess classified material at their facility(ies) where they have an FCL and Cognizant Security Authority (CSA)-approved safeguarding capability at the appropriate level.

Ref 10a. COMSEC: Classified COMSEC material is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. COMSEC access shall be IAW DoD 5220.22-M. When access is required at Government facilities, contractor personnel will adhere to COMSEC rules and regulations as mandated by Command policy and procedures. Written concurrence of the GCA is required prior to subcontracting. Prior approval from the Contracting Officer is required in order for a Prime Contractor to grant COMSEC access to a subcontractor. The Prime Contractor should also notify the National Security Agency (NSA) Central Office of Record before negotiating or awarding subcontracts.

(U) (For Visitor Groups) Contractor will require access to COMSEC information at the on-base locations listed in item 8a. On-base contractors will not require their own COMSEC account. Access will be controlled by Space Base Delta 3 or host installation. On-base contractors will protect COMSEC material IAW directives identified by the installation COMSEC Custodian to include Air Force Manual 17-1302-0, Communications Security (COMSEC) Operations. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances.

Ref 10e(1). National Intelligence Information - Sensitive Compartmented Information (SCI): No public release of information authorized, public disclosure or confirmation of any subject related to the support contract is not authorized without first obtaining written approval from the SSC/S2S Special Security Office (SSO). Written concurrence of SSC/S2S SSO is required prior to subcontracting. The SSC/S2S SSO shall have security cognizance for SCI. All activities involving SCI (including discussions) will be conducted in Sensitive Compartmented Information Facilities (SCIFs). Physical security standards for SCIFs are contained in ICD 705, applicable IC

specifications, or standards and implementing DoD Component policies. See current SCI Addendum.

The contractor shall nominate a Contractor Special Security Officer (CSSO) and Alternate(s) to SSC/S2S SSO through the Government program office Special Security Representative (SSR) or Contracting Officers Representative (COR). CSSO and alternates must be SCI eligible and briefed into SCI.

Ref 10e(2). National Intelligence Information - Non-SCI: The contractor shall handle non-SCI or "collateral" intelligence information IAW Chapter 9, Section 3 of DoD 5220.22-M, NISPOM, DoDM 5200.01-V1-V3, Information Security Program and AFI 16-1404, Air Force Information Security Program. Particular emphasis is placed on the contractor(s) correctly understanding and heeding intelligence portion markings. As classified material, the contractor shall afford collateral intelligence information the same protections, safeguards, and precautions required by any classified material required by DoDM 5200.01-V1-V3, unless special intelligence related handling instructions are specifically imposed. The contractor shall neither disclose nor release intelligence derived information, whether its status is collateral or SCI, without the prior consent of SSC/S2S SSO.

Contractor will require access to intelligence information and must comply with directions provided by the GCA or Contracting Officer's Representative (COR). The Government Program Manager has determined that disclosure does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information. The GCA or COR will identify what intelligence information is required for the contractor to satisfy the contract and will submit that information to the servicing Senior Intelligence Officer (SIO) for approval prior to granting access.

Ref 10f. Special Access Program (SAP) security requirements apply, see current SAP Continuation Pages for guidance.

Ref 10j. Controlled Unclassified Information (CUI): CUI is the term which collectively refers to For Official Use Only (FOUO), Unclassified Controlled Technical Information (UCTI), Unclassified Controlled Nuclear Information (UCNI) and many other designations. CUI information generated and/or provided under this contract shall be managed and safeguarded IAW DoDI 5200.48, Controlled Unclassified Information, which supersedes DoDM 5200.01, Volume 4, DoD Information Security Program. DoDI 5200.48 DAFI 16-1403 Controlled Unclassified Information Implementation Guidance applies to arrangements, agreements, contract, and other transaction authority actions requiring access to CUI according to terms and conditions of such documents, as defined in Clause 2.101 of the Federal Acquisition Regulation (FAR) and Section 2002.4 of Title 32, CFR, including but not limited to, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements.

AFGM2021-16-01 supersedes sections of Air Force Instruction (AFI) 16-1404, Air Force Information Security Program, where the designation For Official Use Only (FOUO) is referenced. See Block 11l for Information Systems protection guidance.

All CUI must be controlled until authorized for public release in accordance with DoDI 5230.09, Clearance of DoD Information for Public Release, DoDI 5230.29, Security and Policy Review of DoD Information for Public Release, DoDM 5400.07, DoD Freedom of Information Act (FOIA) Program, and DoDM 5205.07-V1, DoD SAP Security Manual: General Procedures.

Support to CUI portions of work on a lawful government contract may be accomplished by individuals without a security clearance needing to access CUI. No individual may have access to CUI unless it is determined that the individual has an authorized, lawful government purpose. The individual with authorized possession, knowledge, or control of CUI will determine whether an individual has an authorized, lawful government purpose to access designated CUI. CUI does not include information lawfully and publicly available without restrictions. CUI requires safeguarding measures identified by the necessary law, regulation, or government wide policy with which it is associated.

Reference security requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, they must use the NIST SP 800-171A procedures to evaluate the effectiveness of the tested controls. NIST SP 800-171A is the primary and authoritative guidance on assessing compliance with NIST SP 800-171.

Ref 11c. Receive, Store, and Generate Classified Material: The contractor requires access to classified source data up to and including Top Secret in support of the work effort. Any extracts or use of such data requires the contractor to apply derivative classifications and markings consistent with the source documents. Use of "Multiple Sources" on the "Derived From" line necessitates compliance with the NISPOM, paragraph 4-208a, and the use of a bibliography.

For all performance locations identified in Block 8 on this DD Form 254, the contractor will abide by local government installation/facility policy and procedures for handling classified information. In the performance of this contract, the contractor will reference and abide by the appropriate security classification guidance when generating or deriving classified material or hardware. All classified information received or generated will be properly stored and handled according to the markings on the material. All classified information received or generated is the property of the U.S. Government. At the termination or expiration of this contract, the U.S. Government will be contacted for proper disposition instructions.

Ref 11d. Fabricate, Modify, or Store Classified Hardware: The Contractor is required to provide adequate storage for classified hardware up to and including the level indicated in Block lb. If the hardware is such a size and/or quantity that it cannot be safeguarded in an approved storage container, the use of an approved 'Closed Area' will be required. The Closed Areas need to meet the standards listed in Chapter 5 of the NISP, AFMAN 16-1406 Volume 2, and 32 CFR Part 117 NISPOM. If there are no alarms, then the Closed Areas will have to be checked every 4 hours by contractor security to ensure the integrity of the room. If the contractor does not have an approved Closed Area, then the area will be considered a Restricted Area per Chapter 5 of the NISP, AFMAN 16-1406 Volume 2, and 32 CFR Part 117 NISPOM and the classified material will require 24 hour surveillance.

Ref 11g. Authorized to Use the Services of Defense Technical Information Center (DTIC): Access to DTIC can be requested through the DD Form 1540, Registration for Scientific and Technical Information Services or online at: https://www.dtic.mil/dtic/registration/registration.html.

Ref 11h. Require a COMSEC Account: A COMSEC account must be established when accountable COMSEC material is to be provided, acquired, or produced under a contract. The GCA will inform the contractor that a COMSEC account is required.

(On-base contractors) The contractor will be required to establish and maintain a COMSEC user account following the procedures and requirements contained in Committee on National Security Systems (CNSS) Policy No. 3, National Policy for Granting Access to U.S. Classified Cryptographic Information and AFMAN 17-1302-O, Communications Security (COMSEC) Operations, the NISPOM, installation COMSEC account procedures and/or NSA Policy Manual No. 3-16.

(Off-base contractors) NSA account will be established for and maintained by contractor IAW CNSS Policy No. 3, National Policy for Granting Access to U.S. Classified Cryptographic Information. The Contractor will comply with the additional security requirements and the management of NSA information/material as defined in the manual.

Ref 11j. Have OPSEC Requirements - The contractor shall accomplish the following minimum requirements in support of the SSC/AA Operations Security (OPSEC) Program.

a. The contractor shall protect activities that warrant OPSEC to include but are not limited to research, development, analysis, test and evaluation; acquisitions; treaty verification; nonproliferation protocols; international agreements; force protection operations; special access programs; and activities that prepare, sustain, or employ Military Services over the range of military operations.

b. The contractor shall protect sensitive unclassified information and activities, which could compromise classified information or operations, or degrade the planning and execution of military operations performed by the contractor in support of the mission. Sensitive unclassified information is that information marked For Official Use Only (FOUO), Controlled Unclassified Information (CUI), Privacy Act (PA) Of 1974, Company Proprietary, and as identified by the government program office and program manager, and SSC/AA OPSEC Program Manager. OPSEC is essential to defense activities that may be compromised whenever open sources and detectable activities provide information that when compiled or analyzed is a detriment to U.S. interests.

c. Compliance with security requirements imposed by documents generated in response to DoDI 5200.39, Critical Program Information (f) Identification and Protection within Research, Development, Test and Evaluation (RDT&E).

d. The contractor shall comply with the NSSL OPSEC Plan, and apply protective measures therein. Research and Development contractors (off-base) shall develop an OPSEC Plan in accordance with NSSL OPSEC Plan, AFI, DoDM 5205.2 and as identified by the government program office and program manager, and SSC/AA OPSEC Program Manager. OPSEC shall be a part of ongoing security awareness program conducted in accordance with Chapter 3, Section 1, of the National Industrial Security Program Operating Manual.

e. The contractor shall protect all unclassified information and activities, which could compromise classified information or operations, or degrade the planning and execution of military operations performed by the contractor in support of the mission. Contractor shall protect controlled unclassified information (CUI) and information identified in the SSC and SSC program office critical information list (CIL). Disposition of Critical Information and CUI obtained or produced pursuant to this agreement shall be shredded/degaussed to prevent reconstruction.

f. Disposition of Sensitive Information, Critical Information, FOUO, and PA obtained or produced pursuant to this contract shall be shredded/degaussed to prevent reconstruction. Email transmission of Sensitive Information, Critical Information, FOUO, and PA obtained or produced pursuant to this contract will be encrypted or password protected. In addition, email containing FOUO and PA shall be marked in the subject line with (FOUO) or (PA). CUI shall also be included at the beginning of the email with a non-disclosure statement.

Ref 11k. Be Authorized to Use Defense Courier Service (DCS):

The contractor is authorized to use the services of DCS. Contractor shall comply with Part 117 of Title 32, CFR, NISPOM, for authorized use of DCS and obtain GCA authorization as required. Written concurrence from the GCA is required prior to subcontracting.

Go to https://www.ustranscom.mil/cmd/associated/dcd/ for DCS points of contacts and guidance. Written GCA approval is required before

a prime contractor can authorize a subcontractor to utilize DCS.

Ref 11l. Receive, Store, or Generate Controlled Unclassified Information (CUI):

Protection of Unclassified DoD Information on Non-Government Information Systems: The Contractor must comply with the information safeguards as specified in DoDI 8582.01, Security of Unclassified DoD Information on Non-DoD Information Systems, CNSS Policy No. 18, National Policy on Classified Information Spillage, Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01, Information Assurance and Support to Computer Network Defense (CND), and Air Force Manual 17-1301, Computer Security.

The Contractor shall comply with Defense Federal Acquisition Regulation (DFAR) Clauses related to the Disclosure of Information (DFAR 252.204-7000), Safeguarding Covered Defense Information and Cyber Incident Report (DFARS 252.204-7012 and DFAR Subpart 204.73) for the protection of unclassified controlled technical information. In line with this clause, NIST SP 800-171 provides guidance for the protection of CUI on non-federal information systems.

Contractor shall apply security controls contained in NIST SP 800-171 for the protection of CUI on non-DoD information systems. CUI information will not be placed on publicly accessible web sites.

Definitions:
Adequate Security - Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information (see OMB Circular A-130). Current means of achieving adequate security for Information Technology is to use DoD, CNSS and NIST guidance (see CNSS Instruction No. 4009).

Non-Sensitive Information - Information available in the public domain or DoD information that has been approved for public release.

Sensitive Information - Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code, "The Privacy Act" but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Ref 11m. In order to perform assigned duties, the contractor will need access to various government systems as identified by the GCA. The contractor shall follow overarching, and local requirements for access to these systems. Contractors shall be held accountable for actions they initiate on the network and shall conduct business IAW USSF, USAF, SSC, and host installation instructions and policies. The contractor shall not access, download or further disseminate any information/data (i.e., intelligence, NATO, COMSEC, etc.) outside the execution of the defined contract requirements and without the guidance and written permission of the GCA. In the event that any additional access is required, the GCA must modify the contract requirements, and revise the DD Form 254. Note: Once the GCA has modified the requirements for the generation of a revised DD Form 254, the Contractor must complete the Access Request Form(s), along with the modified DD Form 254, and forward to the GCA prior to receiving access. A NATO awareness brief will also be required for all Contractors prior to access to the NATO accredited terminals. Written concurrence of the GCA is required prior to subcontracting.

Secret Internet Protocol Router Network (SIPRNET) Access - Access to SIPRNET by contractor at government locations will be IAW applicable guidance and policies. Access to SIPRNET will be IAW DoDI 8500.01, Cybersecurity, and Risk Management Framework (RMF) for DoD Information Technology.

The terms Cybersecurity, Information Systems, and Information Technology are defined in CNSS Instruction No. 4009 and Cybersecurity DoDI 8500.01.

Unauthorized Disclosure: Government and contractor personnel must act to protect Technical Program design, development, or manufacturing data under their control from unauthorized disclosure to any foreign person or a U.S. person residing in a foreign country. Government and contractor organizations must inform the U.S. State Department under the provision of the ITAR regarding any unauthorized disclosure.

Pre-contract award access to classified is not required.

Ref 13: Security Guidance

Public release of Special Access Program (SAP) related data is not authorized without prior coordination through the Office of Special Investigation (OSI), Office of Special Projects (PJ) Security Director and subsequent approval of the Original Classification Authority (OCA) and the Air Force Special Access Program Central Office (AF SAPCO). Submit all proposed public disclosures related to SAP data to the Government Program Manager and the OSI PJ Program Security Officer (PSO).

Program Protection Plans (PPP) and Security Classification Guides (SCG): The contractors shall protect Critical Program Information (CPI) and Critical Components (CC), technologies and systems in compliance with the current Contractor version of the PPIP and the NSSL program version of the PPP. Program Security Classification Guides (SCGs) will be provided by the Government program office. Classified national security information, and unclassified controlled information (CUI) shall be protected as outlined in the SCG, NISPOM, DODM 5200.01 V1-3 and DoDI 5200.48.

Contractors shall develop a Program Protection Implementation Plan (PPIP) to be approved by the Government program office. The PPIP shall describe the protection measures being implemented by the contractor and sub-contractors for CPI and CC. The prime contractor shall flow-down to any subcontractor protection requirements for implementation as described in the PPIP in compliance with NSSL PPP. The Government program office shall conduct Program Protection Surveys at contractor locations to assess the effectiveness of the established PPIP.

(U) The following website address for both DoD issuances and e-publishing:
DoD issuances: https://www.dtic.mil/whs/directives/
AF epublishing: https://www.e-publishing.af.mil/

Personnel Security - For access to classified information, the contractor will ensure all required actions IAW DoDM 5200.02, April 3, 2017 Change 1, October 29, 2020 and 32 CFR Part 117, are completed for personnel working on this contract. An interim SECRET or CONFIDENTIAL Personnel Security Clearance (PCL) is valid for access to classified information at the level of the eligibility granted. Interim SECRET or CONFIDENTIAL PCLs are authorized except when the contractor will require access to COMSEC information, Restricted Data, or NATO information, where a finalized security clearance is required. Note, an interim TOP SECRET PCL is the equivalent of a final SECRET PCL. Security clearances are in accordance with the NISPOM. Access to SCI will be in accordance with the current SCI Addendum and DoD Manual 5105.21 Volumes 1-3 for SCI management. Contractor(s) will not be afforded access to classified information at any level (i.e., Confidential, Secret, or Top Secret) until the Department of Defense Consolidated Adjudications Facility (DoD CAF) grants a final PCL at the appropriate level. Interim PCLs are authorized only when granted by the adjudicative authority and have been entered into Defense Information System for Security (DISS). Contractor(s) must be employed in a position that requires a clearance in order to be submitted for the appropriate PCL. Contractor(s) Facility Security Officer (FSO) will submit all investigation requests through Defense Information System for Security (DISS) and ensure individuals complete a clearance application in the Electronic Questionnaires for Investigations Processing (e-QIP). Contractor(s) FSO reviews, approves, and forwards the completed e-QIP to Defense Counterintelligence Security Agency (DCSA) Vetting Risk Operations Center (VROC) for approval, issuance of an interim clearance, and release to Office of Personnel Management (OPM) for investigation. Alternate methods of clearance submission are acceptable as long as the contractor security personnel ensures clearance levels are available in Defense Information System for Security (DISS) for review.

Contract performance on a Government installation and/or 1) access to classified information, and/or 2) IT Level I/II/III access is required, and/or 3) when a security clearance is required to perform unclassified services in a facility requiring a security clearance for unescorted access, shall undergo a Personnel Security Investigation (PSI), as appropriate. This is also applicable to contractor and subcontractor personnel who are visiting or on a temporary and/or escort duties for a period of 90 days or more. This requirement is for personnel who have or may need access to restricted or controlled areas. Contractor employees who require access to government IT systems/networks are determined to be trustworthy by the completion of a favorable PCL investigation appropriate with assigned duties and by a designated government official prior to IT access being granted. This is accomplished through the system authorization access request, DD Form 2875, process. Reference AFI 31-501, Personnel Security Program Management (or applicable revisions) for background investigation requirements.

Reference AFI 16-1406, Air Force Industrial Security Program and AFI 31-101, Integrated Defense, for administrative approaches to identify installation access for contractors as “Visitor Groups”, “Intermittent,” and “Cleared Facilities.” Both installation and network access as prescribed in AFI 16-1406 correlates to AFI 36-3026, Volume 2, Common Access Card (CAC), for contractor and volunteer populations, eligibility and enrollment to DEERS via the online TASS application.

Grant contractors (prime contractors and subcontractors) access to the installation IAW AFMAN 31-113, Installation Perimeter Access Control.

Any conflict and/or issue regarding classification level between this and any other application guide will be protected at the highest level until the conflict or issue is resolved by the Program Security Officer (PSO), SSC/AA Security Manager, Information Protection Office (IPO) and Special Security Office (SSO). Written resolution and/or direction will be provided by the PSO, SSC/AA Security Manager, IPO and SSO.

Security Incident Reporting - In addition to the reporting requirements directed by the NISPOM, the contractor shall provide a concurrent report of loss or compromise and/or unauthorized access of CUI, FOUO, and any classified information, materials, hardware, and/or systems to the GCA, Government Information System Security Manager (ISSM), SSC/AA Security Manager, and Information Protection Office (SSC/BZS), and supporting Cognizant Security Office (CSO) (DCSA, etc.). Contractor shall report loss or compromise and/or

unauthorized access of CUI, FOUO, and any classified information, materials, hardware, and/or systems to the CSO identified in Block(s) 6c and 8c.

Upon expiration of this contract, the contractor shall request disposition instruction for all classified and unclassified project material. The contractor may be directed to properly destroy or return material. If the contractor desires to retain classified or unclassified program information, the contractor must provide a request six (6) months in advance of contract completion to transfer project information to follow-on contractor or similar effort, contractor must have written approval from the Government Program Manager, GCA and SSC/AA Security Manager. The contractor shall return to the GCA all CACs, security badges, entry passes/vehicle decals issued to contractor personnel. This applies to termination, cancellation and/or expiration contract, and/or of employment and/or suspension of clearance.

Transfer of document to other Independent Research and Development (IRAD) is not permitted.

The undersigned has reviewed the Security Specification, understands the provisions and will ensure that it is complied with within the limits of his/her responsibility, and that any violations are brought to the attention of the GCA.

Government Program Manager: Lt Col Nicholas Longo, SSC/AAM, (310) 653-3090, nicholas.longo.1@spaceforce.mil

GCA/Contracting Officer: Ms. Kirsten Prechtl, SSC/AAK, (310) 653-3696, kirsten.prechtl@spaceforce.mil

Security Manager: Mr. Nicholas Alvarez, SSC/AA, (310) 653-1227, nicholas.alvarez.2@spaceforce.mil

Chief, Information Protection Office: Mr. Reginald King, SSC/BZS, (310) 653-1254, reginald.king.1@spaceforce.mil

Chief Industrial Security: Ms. Sharon Jones, SSC/S2S SSO, (310) 653-0988, sharon.jones.15@spaceforce.mil

Program Security Officer: Mr. Malcolm Jones, OSI/PJ Det 7 OL-A, (310) 416-1555, malcolm.jones.5@us.af.mil

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
SSC/AAM	Program Manager	
SSC/AAK	Contracting Officer	
SSC/AA	Nicholas Alvarez Security Representative	
SSC/BZS	Reginald King Industrial Security Specialist	
SSC/S2S SSO	Sharon M. Jones, Chief, Industrial Security	
OSI/PJ	Malcolm L. Jones PSO, OSI/PJ Det 7 OL-A	

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.)

1. (U) See current SCI Addendum.
2. (U) Program Protection Planning: The prime contractor and its subcontractors shall protect Critical Program Information (CPI), Critical Components (CC), technologies and systems when identified in the NSSL Program Protection Plan (PPP).
3. (U) For OPSEC requirements (reference Block 13 for details). Contractor will comply with the policies and procedures outlined in the NSSL OPSEC Plan in support of this effort. NSSL OPSEC Plan will be furnished by the government upon contract award to ensure compliance with all OPSEC guidelines set forth.
4. See NSSL OPSEC Plan.
5. Ref 10f: SAP security requirements apply, see current SAP Continuation Pages for details.

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.)*

The DCSA is relieved of security inspection responsibility for contract performance on government installations. The Commander retains cognizance over contracts on the installation. SSC Information Protection Office staff is designated as a member of the Wing Inspection Team and has inspection authority when assigned under SSC/IG.

SCI security requirements apply, see current SCI Addendum for details.

SAP security requirements apply, see current SAP Continuation Pages for details.

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

a. GCA NAME
SSC/AAK

b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)*
FA8811

c. ADDRESS *(Include ZIP Code)*
483 N. AVIATION BLVD.
EL SEGUNDO, CA 90245

d. POC NAME
Kirsten Prechtl

e. POC TELEPHONE *(Include Area Code)*
+1 (310) 653-3696

f. EMAIL ADDRESS *(See Instructions)*
kirsten.prechtl@spaceforce.mil

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)*
Kirsten Prechtl

b. TITLE
CONTRACTING OFFICER

c. ADDRESS *(Include ZIP Code)*
SSC/AAK
483 N. AVIATION BLVD.
EL SEGUNDO, CA 90245

d. AAC OF THE CONTRACTING OFFICE *(See Instructions)*

e. CAGE CODE OF THE PRIME CONTRACTOR *(See Instructions.)*

f. TELEPHONE *(Include Area Code)*
+1 (310) 653-3696

g. EMAIL ADDRESS *(See Instructions)*
kirsten.prechtl@spaceforce.mil

h. SIGNATURE

i. DATE SIGNED *(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.)*
SSC/BZS, SSC/S2S SSO, SSC/SAPMO, and SAF/AAZ (via OSI/PJ)