PERFORMANCE WORK STATEMENT (PWS)

FOR

CIVILIAN GUARDIAN COURSE (CGC)
CURRICULUM DEVELOPMENT AND ITERATION

29 June 2026

STARCOM
Delta 1

Template AO: HQ STARCOM/Program Management

STATEMENT D: Distribution authorized to the Department of Defense and U.S. DoD Contractors only; administrative/operational use; 13 August 2021. Other requests for this document shall be referred to HQ STARCOM Program Management.

WARNING: This document contains technical data whose export is restricted by the Arms Export Control Act (Title22, USC, Sec 2751, et. seq.) or the Export Administration Act of1979, as amended, Title 50, USC., App. 2401, et.seq. Violations of these export laws are subject to severe criminal penalties. Dissemination of this document is controlled under DoD Directive 5230.25.

DESTRUCTION NOTICE: Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

CHANGE CONTROL SUMMARY

Revision (Rev). *A revision should be used to consolidate all changes into a new basic document with a new basic date. It should be used to clean up the document when it begins to become confusing with too many changes. It is the Data Managers (DM) decision when to revise the document. Number the revision and include a summary of the revisions in the change table. DM will remove all change bars when the document is revised since the revised document takes all previous changes into account. Do not remove changes from the change table when the document is revised since they may lend important historical value.*

Version (Ver). *A change that is administrative in nature does not require the document to be re-staffed. Changes that remove or add items periodically assessed or affect items assessed in frequency of assessment or thresholds must be re-staffed for approval. Consolidate changes when possible. Include a summary of the changes incorporated in the change table. Ensure change bars have been inserted after initial release.*

Rev./Ver.	*Eff. Date*	*Description*
6.3	29 Apr 26	Version for SAM use. Added in missing sections. Consolidated deliverables.
6.4	1 May 26	Edited following comments on 6.3
6.5	29 Jun 26	Removed curriculum GFIs due to confirmed unavailability, corrected Services Summary references

Table of Contents

1. Introduction/Background 1
1.1. Mission Overview 1
1.2. Scope 2
2. General Requirements 3
2.1. Non-Personal Services 4
2.2. Contractor Management 4
2.2.1. Contract Administration 4
2.2.2. Contractor POC 5
2.2.3. Personnel Administration 5
2.2.4. Contractor Identification 5
2.3. Contractor Personnel, Disciplines, and Specialties 5
2.3.1. Personnel Turnover 8
2.3.2. Removal of Personnel at Government Request. 8
2.4. Location and Hours of Work RESERVED 9
2.4.1. Building Access RESERVED 9
2.4.2. Morale Events RESERVED 9
2.4.3. Closures RESERVED 9
2.4.4. Teleworking RESERVED 9
2.5. Travel / Temporary Duty (TDY) RESERVED 9
2.6. Security and Safety 9
2.6.1. DD Form 254 9
2.6.2. Operational Security (OPSEC) RESERVED 9
2.6.3. Controlled Unclassified Information (CUI) 9
2.6.4. Special Access Programs (SAP) RESERVED 10
2.6.5. Personnel Security Program RESERVED 10
2.6.6. Non-Disclosure Agreements (NDA) 10
2.6.7. Communications Security (COMSEC) Monitoring 10
2.6.8. Counterintelligence Cooperation RESERVED 10
2.7. Manpower Reporting 10
2.8. Documentation 11
2.8.1. Documentation Rights 11
2.8.2. Government Data 11

2.8.3. Quality Control 11
2.9. Performance Evaluation. 13
2.10. Government Furnished 14
2.10.1. Government Furnished Property (GFP). 14
2.10.2. Government Furnished Resources. 14
2.10.3. Government Furnished Information (GFI) 14
2.10.4. Materials and Other Direct Costs (ODC) 14
3. Performance Requirements 14
3.1. Transition 15
3.2. Associate Contractor Agreements (ACA) RESERVED 15
3.3. STARCOM Directed Meetings/Events 15
3.3.1. Kick-Off Meeting 15
3.3.2. Program Management Review (PMR) RESERVED 16
3.3.3. Working Group Tag ups 16
3.4. Civilian Guardian Course Descriptions and Requirements 16
3.4.1. The Contractor shall design, develop, and sustain all course materials—including lesson plans, instructional aids, student/instructor guides, and associated assets—throughout the period of performance Working Group Tag ups 18
3.4.2. Course Feedback 20
3.4.3. The Contractor shall provide Multimedia support to CGC Government personnel in all necessary multimedia activities used throughout CGC curriculum build. Multimedia support includes the design, development, and production and deployment of multimedia products for use in CGC 20
3.4.4. Courseware Documentation 21
4. Applicable Publications 22
5. Deliverables 23
6. Services Summary 26
Attachment 1 – Government Furnished Information 28
Attachment 2 – Tentative CGC Objectives 29
Attachment 3 – CGC Tentative Sequencing & Pacing for Online Modules 47
Attachment 4 – CGC Tentative Sequencing & Pacing for Capstone Portion 49
Attachment 5 – Notional Learning Experiences and Assignments 51
Attachment 6 – Part 5352 - Solicitation Provisions and Contract Clauses 54
Attachment 7 – CMMC 60

Performance Work Statement (PWS)

1. Introduction/Background

The Officer/Enlisted/Civilian (O/E/C) Principles and Narratives set the foundation for how each member of the United States Space Force (USSF) contributes to space superiority. To support this structure, dedicated training programs were established for officers and enlisted personnel. However, a specific developmental course for Civilian Guardians—who comprise over one-third of the total force—was missing from this triad. This gap resulted in an inconsistent onboarding process, impacting the speed of mission integration and posing a risk to long-term civilian talent retention.

This gap led to the creation and execution of three prototype courses in Los Angeles, Colorado Springs, and the National Capital Region to test content and curriculum based on guidelines provided by USSF/S1 and STARCOM. The purpose of this Statement of Work is to implement the evolved and formalized training model developed from these prototypes: the Civilian Guardian Course (CGC).

That feedback has been synthesized by the Government into the course objectives (Attachment 2) and the sequencing and pacing attachments (Attachments 3–4), which together constitute the complete expression of the resulting design intent. To preserve the integrity and spirit of this foundation, the finalized curriculum must achieve the following course-design priorities:

- Foster Guardian Identity and Mission Alignment: Deepen students' understanding of the USSF mission and national security role, strengthening their sense of purpose, commitment, and connection to Guardian values.
- Embed a Strategic Warfighter Perspective: Actively bridge the gap between tactical, day-to-day tasks and overall strategic objectives.
- Facilitate High-Level Engagement: Integrate dedicated time and structured interactions with USSF senior leaders and Subject Matter Experts (SMEs).
- Build Professional Networks: Provide deliberate opportunities for students to discover the broader USSF structure, forging strong collaborative networks across Deltas and Field Commands.

1.1. Mission Overview

The mission of the Civilian Guardian Course (CGC) is to serve as the foundational developmental experience for new Civilian Guardians. It is designed to accelerate their transformation into mission-focused professionals, providing the operational stability, unit continuity, and depth of expertise necessary to support Joint Warfighting functions and U.S. National Security.

The CGC is structured to guide new Civilian Guardians into becoming fully integrated, space-minded, warfighting Guardians. The CGC begins by establishing a foundational space-minded

perspective, requiring graduates to analyze the strategic environment to understand the 'why' behind the USSF mission. From there, it builds towards forging the Guardian identity by examining how USSF doctrine and Guardian warfighting ethos define their unique role and responsibilities and shape their impact as a civilian Guardian. The course then advances from theory to application, challenging students to apply concepts to solve complex, simulated operational challenges. By the conclusion of the course, each Guardian will have constructed a personalized development plan. This final step transforms the course from a singular training event into the starting point of a career-long journey, directly linking personal growth to USSF strategic needs and serving as a powerful tool for talent retention.

1.2. Scope

This effort shall be for the initial design and full development of assigned CGC classes/lessons, corresponding instructor guides, and all student-facing training materials as described in this PWS. The Contractor shall work in tandem with the GOV who will be simultaneously developing the inherently governmental curriculum to ensure continuity and branding consistency. While both parties will collaborate to integrate the final course, the Contractor is solely responsible for authoring and developing all original instructional content for their assigned lessons. All contractor-developed materials, including but not limited to lessons, activities, templates, and assessments, are subject to formal Government review and approval prior to implementation. Delivered over a two-month period, CGC is a cohort-driven, interactive course that uses a blended learning model.

The initial online phase shall consist of a 40-hour online curriculum, comprising a mix of synchronous and asynchronous engagements. This phase shall be developed as a high-engagement, multi-modal experience rather than a collection of static lectures or slide presentations. These 40 hours shall encompass the total student effort required to complete the curriculum, such as: mandatory readings, instructional video engagement, independent assignments and other knowledge assessments, online synchronous group collaboration, and direct synchronous (online or offline) interaction with the instructor and other SMEs. The course culminates in a one-week residential capstone focused on high-fidelity, performance-based activities, including instructor-led simulations. See Attachment 2 - 5 for KTR vs GOV curriculum responsibilities/assignments.

The Contractor will be required to participate in all curriculum development and iteration efforts from pre-execution through post-execution. The Contractor shall be responsible for the complete build-out and technical configuration of all assigned course content within the Government-provided Learning Management System (LMS). Curriculum maintenance and updates will occur on a consistent and reoccurring schedule as part of this effort. Additionally, this PWS covers all required multi-media support and Instructional Systems Design (ISD) support for the performance period outlined in this PWS. The Government retains final authority on all course content, instructional methodologies, and learning activities.

2. General Requirements

This section describes the general requirements for this effort. The following sub-sections provide details of various considerations on this effort.

The CGC is an 80-hour blended learning program designed to integrate foundational knowledge with high-impact practical application. The course architecture is composed of two distinct phases: Phase I consists of multiple online modules delivered over a 20-business-day window using a hybrid of synchronous and asynchronous modalities. This online portion is distributed intermittently, and while the exact schedule is not yet finalized, the contractor must maintain the flexibility to support this spread-out timeline. Phase II is the immersive engagement which serves as the course culmination, utilizing an in-person, experiential environment to tie together all aspects of the CGC curriculum.

The contractor shall provide curricular support for two prototype offerings during the period of performance. Iteration of course content and related materials will take place throughout the period of performance. Further details of the course descriptions and needed work are listed in Section 3 of the PWS.

The **Period of Performance** is as follows: Contract Start – 14 May 2027

The development of the curriculum is designed to be cyclical and iterative, involving an initial delivery for a validation pilot, followed by iterative refinement based on feedback.

A "Complete Deliverable Package" for each module is defined as all of the following components, fully integrated and operational on the designated Learning Management System (LMS):

- Student-facing content
- Instructor-facing content
- All associated feedback mechanisms for content feel and learning assessment (e.g., quizzes, surveys, assessments, answer keys, rubrics, etc.)
- Any and all supplementary or supporting materials

Schedule of Deliveries

The project will adhere to the following phased delivery schedule.

Phase 1: Initial Curriculum Delivery. The Complete Deliverable Package for Contractor assigned online and capstone content is due NLT 30 November 2026.

Phase 2: Iteration of content. The iteration process is intended to be continuous. For each module, the analysis of student feedback and subsequent content iteration shall begin as soon as that specific module's validation pilot is complete and feedback becomes available. This work should not be postponed until all modules have completed their initial pilot. An iterated and updated version of

online the Complete Deliverable Package, incorporating all feedback, shall be delivered NLT 12 Mar 2027.

Phase 3: Final Revisions and Project Completion. Following the delivery of each iterated module during the second pilot, any subsequent changes and updates requested based on a final review must be completed. All project activities and final revisions are to be concluded by the end of the period of performance, 14 May 2027.

2.1. Non-Personal Services

The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances will the Government assign tasks to, or prepare work schedules for individual Contractor employees. The Contractor shall ensure its employees understand the prohibitions imposed on the Government regarding personal services contracts, as defined in the FAR as "*a personal services contract is characterized by the employer-employee relationship it creates between the Government and the contractor's personnel."* The Contractor shall manage its employees and guard against any actions that are of the nature of personal services, or give the perception of personal services. If the Contractor believes that any actions constitute, or are perceived to constitute personal services, the Contractor shall notify the Procuring Contracting Officer (PCO) immediately.

2.2. Contractor Management

The Contractor shall integrate and coordinate all activity needed to satisfy the requirement. The Contractor shall manage the timeliness, completeness, and quality of problem identification, and resolution, as applicable. The Contractor shall provide corrective action plans, proposal submittals, timely identification of issues, and effective management of subContractors. The Contractor shall seek to ensure customer satisfaction and professional and ethical behavior of all Contractor personnel. If the Contractor has any proposed revisions to this PWS or any other contract attachment, for the purposes of making the documents more accurate (regulatory changes) or complete (for clarity), the Contractor shall submit suggested revisions as word document with tracked changes and a change request to the COR and CO for consideration.

The Contractor shall provide a Monthly Status Report (MSR) covering activities of the preceding month.

Deliverable

A001 – Monthly Status Report (MSR)

2.2.1. Contract Administration

The Contractor shall ensure its personnel do not perform inherently Governmental activities, as defined in FAR 7.5. The Contractor shall ensure its personnel do not attempt to represent the Government of the United States (US) to any other person or entity, US, or foreign, except for delivering a Government-approved message or position. All briefings, policies, plans and other

formal products the Contractor develops, reviews, and creates, will be reviewed and approved by the Government.

2.2.2. Contractor POC

The Contractor shall have a single point of contact between the Government and Contractor personnel assigned to support this contract. This lead shall coordinate with the Contracting Officer's Representative (COR) to obtain and clarify contract requirements and shall be responsible for the daily control and supervision of the Contractor's employees.

2.2.3. Personnel Administration

The Contractor shall maintain the currency of their employees by providing initial and refresher training as required to meet the PWS requirements. The Contractor shall obtain approval from Government prior to attending Government-provided training classes. Provided there is no cost to the Government, the Contractor may be eligible to attend Government-sponsored and Government-provided training to maintain proficiency in software, administrative procedures or other areas. Additionally, provided there is no cost to the Government, the Contractor may be eligible to attend third-party-provided off-site seminars and classes.

2.2.4. Contractor Identification

Contractor employees shall clearly identify themselves as "Contractors" at all times, in all communications and representations, including in the workplace, at meetings, in conversations, telecommunications, mail, electronic mail (e-mail), and faxes, whether with Government personnel, other Contractor personnel, or with the public. Contractor personnel shall wear a readily visible badge that clearly identifies them as Contractor employees.

Deliverable

A002 – Contractor Personnel Roster

2.3. Contractor Personnel, Disciplines, and Specialties

The Contractor shall accomplish the assigned work by employing and utilizing qualified personnel with appropriate combinations of education, training, and experience. The Contractor shall ensure the labor categories, labor rates, and man-hours utilized in the performance of each Task Order (PWS line item) issued hereunder will be the minimum necessary to accomplish the task. The Contractor shall provide the necessary resources and infrastructure to manage, perform, and administer the contract.

Substitutions not meeting the exact criteria below may be approved by the COR on a case-by-case basis. The Contractor must submit a written justification demonstrating equivalent expertise and experience.

Role	**Minimum Required Skills/Education/Experience**	**Highly Desired Skills/ Education/Experience**
Contract Program Manager	Master's degree in Business or Program Management or six (6) years of experience as a Program Manager Excellent Soft skills; familiarity with engaging multiple DoD agencies / organizations (e.g., SMC, HQ USSF, NRO, Intelligence Community (IC) as well at multiple levels (e.g., Section, Division,)	• Eligible for a Common Access Card (CAC) / Favorable Tier 1 Background Investigation (NACI) • Project Management Professional Certification or 6 years of experience as a Program Manager.
Multi-Media specialist	Bachelor's Degree in Multimedia, or a related field or combination of lower degree and experience in related field.	• Eligible for a Common Access Card (CAC) / Favorable Tier 1 Background Investigation (NACI) • 3+ years of experience with creative design software tools building 2D/3D animations with motion graphics with video production, special effects and sound design while using Adobe Creative Cloud Suite and/or Autodesk's 3DS Max, Maya, or similar • Knowledge of instructional design, eLearning authoring tools, and delivery methodologies • Research and recommend cutting edge technologies and tools to enhance design and development practices
Instructional System Design Specialist	Bachelor's degree in Adult Education, Blended Learning, Instructional Design, or a related field; or, six (6) years of experience in curriculum development for adults or a related	• Eligible for a Common Access Card (CAC) / Favorable Tier 1 Background Investigation (NACI)

	field or combination of lower degree and experience in related field.	• 3 years of experience in blended learning curriculum/lesson development and instruction • Master's degree in Adult Education or Instructional Design • 3+ years of experience designing and delivering online/blended learning tailored specifically for adult, professional, or military audiences. • Proven ability to collaborate with highly technical Subject Matter Experts (SMEs) to translate complex content into pedagogically sound, accessible online learning modules
Space Subject Matter Expert	Master's degree in Space Studies, Space Policy, Space Ecosystems, or a related field; or eight (8) years of relevant experience in the space domain areas related to course objectives. Demonstrated expertise in topics such as: the global space ecosystem, space sustainability (debris mitigation, STM), national/international space programs, space economies/commercialization, space history, and orbital regimes/assets.	• Eligible for a Common Access Card (CAC) / Favorable Tier 1 Background Investigation (NACI) • Experience synthesizing and communicating complex space concepts to non-technical adult audiences in an educational setting • Demonstrated expertise in adult learning theory (andragogy), curriculum development, and educational technology • 3+ years of experience designing and delivering

		online learning for adult/professional audiences • Experience collaborating with SMEs to develop effective online learning experiences • National or international recognition as a thought leader in areas such as space policy, space sustainability, or the space economy, as evidenced by published research, invited speaking engagements, or advisory roles to government, industry, or academia • Ph.D. or equivalent terminal degree in Space related topics

2.3.1. Personnel Turnover

The Contractor shall ensure continuity of services during personnel absences due to sickness, leave, and voluntary or involuntary termination from employment such that impact to the Government is minimal. Once the Contractor knows an employee will no longer support the requirement, the Contractor shall provide written documentation to the CO and COR within three (3) business days. In this notification, the Contractor shall include the date and time the position will be vacant, anticipated fill date, and what management actions the Contractor will take to ensure uninterrupted performance. Position vacancies shall not exceed 14 calendar days unless approved in writing or otherwise directed in advance by the CO (e.g. a grace period associated with new awards and PWS modifications increasing the number of personnel on a task order).

2.3.2. Removal of Personnel at Government Request.

The Government may request removal (permanent or temporary) of personnel for security, safety or health reasons, or when Contractor personnel behave in an unprofessional manner that would be considered unacceptable by a reasonable person.

2.4. Location and Hours of Work RESERVED

2.4.1. Building Access RESERVED

2.4.2. Morale Events RESERVED

2.4.3. Closures RESERVED

2.4.4. Teleworking RESERVED

2.5. Travel / Temporary Duty (TDY) RESERVED

2.6. Security and Safety

All Contractor personnel proposed to work on this task order must be U.S. citizens. All Contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable National Agency Check (NAC).

The Contractor shall ensure employees who terminate their services to this contract shall immediately return any Government identification/access badges issued in support of this contract. The contractor shall immediately notify the COR of the employees' departure to ensure all access to Government systems and facilities is terminated and update the Contractor Personnel Roster (A002).

If necessary, Contractor employees shall be capable of obtaining and possessing a DoD CAC and an Access ID Badge as required for access to government systems or government facilities in the performance of this contract. Contractor shall use the card IAW AFFARS 5352.242-9001. Upon favorable review, and initiation of the Personnel Security Investigation (PSI) to establish the suitability of an employee for the job and the approval for temporary Automated Information System (AIS) access pending final adjudication of the PSI, the Contractor shall submit to a Contractor's onsite System Manager's request for the DoD CAC and ID Badge.

2.6.1. DD Form 254

The DD Form 254 specifies overarching security requirements and Contractor access to classified information. Course material will be at the UNCLASSIFIED level. No DD Form 254 will be required.

2.6.2. Operational Security (OPSEC) RESERVED

2.6.3. Controlled Unclassified Information (CUI)

The Contractor shall safeguard all information provided and marked as CUI via this contract IAW DoD Instruction (DoDI) 5200.48, Controlled Unclassified Information (CUI). If the Contractor generates/handles any CUI or Federal Contract Information (FCI), it shall protect and disseminate that information per the controls required by DoDI 5200.48 and the Cybersecurity Maturity Model Certification (CMMC) program (described in USC Title 32 CFR §170.3, see

Attachment 7). The Contractor shall monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. The Contractor shall immediately report the potential classification of aggregated or compiled CUI to the CO and the COR. The Contractor shall safeguard unclassified nonpublic information by applying specified network security requirements, as defined in DoD Instruction 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information, which includes identified CUI and Federal Contract Information that resides in or transits contractor unclassified information systems.

2.6.4. Special Access Programs (SAP) RESERVED

2.6.5. Personnel Security Program RESERVED

2.6.6. Non-Disclosure Agreements (NDA)

The Contractor's assigned personnel shall complete and sign Non-Disclosure Agreement(s) (SF-312) regarding protection of sensitive Government and third-party Contractor information.

Deliverable

A002 - Contractor Personnel Roster

A003 - NDA

2.6.7. Communications Security (COMSEC) Monitoring

Telecommunications networks are continually subject to interception by unfriendly intelligence organizations. All communications within DoD organizations are subject to Communications Security (COMSEC) review. The Government may conduct COMSEC monitoring and recording of electronic or voice communications originating from or terminating at DoD organizations at any time. The Contractor shall ensure all assigned personnel are aware that any time they communicate to or from a Government facility, they are subject to COMSEC procedures. The Contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with Government information.

2.6.8. Counterintelligence Cooperation RESERVED

2.7. Manpower Reporting

In accordance with FAR 52.204-14 Service Contract Reporting Requirements, the Contractor shall report all Contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The Contractor shall fill in all required data fields at the data collection site. Use the following web address: www.sam.gov.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, the Contractor shall report all data no later than October 31 of each calendar year. Contractors may direct questions to the System for Award Management (SAM) help desk.

2.8. Documentation

The Contractor shall make all information and documentation generated or maintained (to include Government-furnished documents) by this contract available for Government review upon request for the duration of the contract. The Contractor shall generate and maintain all such documentation in an electronic, editable (where appropriate) format. Contractor-generated format is acceptable, unless otherwise noted by this PWS.

The Contractor shall provide responses to requests for information. These requests are in addition to Deliverable submissions and other documentation that is available for review by request. Requests may cover the range of activities under this PWS.

2.8.1. Documentation Rights

The Government has unlimited rights to data for all deliverables developed under this PWS. The Contractor shall not use any materials pertaining to this contract for business development or any other Contractor purposes; however, the Contractor is authorized to include summary performance information in proposals to be submitted to the Government to satisfy past performance information requirements.

All products developed and produced by the Contractor in the performance of this PWS are the property of the Government, and this could include software, electronic files, hard copy documents, etc. Rights to all documentation are governed by Defense FAR Supplement (DFARS) 252.227-7032, Rights in Technical Data and Computer Software.

2.8.2. Government Data

The Contractor shall request Government approval prior to the use of any proprietary data or software tools to fulfill the requirements of this contract. The Government will provide the Contractor access to information required to accomplish assigned tasks commensurate with security clearance and on a need-to-know basis. The Contractor shall not retain classified or unclassified material generated or received under this contract after the contract ends without approval of the Contracting Officer.

2.8.3. Quality Control

The Contractor shall develop, implement, and maintain a comprehensive inspection system that assures compliance with all requirements of this contract.

The Contractor shall develop a Quality Control Plan (QCP) that demonstrates how the Contractor shall maintain an inspection system acceptable to the Government covering the

services under this contract to include deliverable requirements. The QCP will include procedures to identify, prevent, and ensure non-recurrence of defective services that inhibit or negatively impact the Delta 1 missions.

The Contractor's QCP is the means by which the contracting company providing the product or services reaffirms internally that the work complies with the requirement of the contract.

The QCP shall demonstrate the Contractor’s documented processes and procedures to monitor and control:

- Objectives for Services Summary Items
- Non-conformances

The draft finalized QCP will be provided to the government within 30 days after award for potential acceptance and review. It will be accepted, if deemed adequate to prevent or correct defective services as described above. The CO may notify the Contractor of required modifications to the plan during the period of performance. The Contractor then shall coordinate suggested modifications and obtain acceptance of the plan by the CO. Any modifications to the program during the period of performance shall be provided to the Contracting Officer for review no later than 10 working days prior to effective date of the change. The QCP shall be subject to the Government's review and approval. The Government may find the QCP "unacceptable" whenever the Contractor's procedures do not accomplish quality control objective(s). The Contractor shall revise the QCP within 10 working days from receipt of notice that QCP is found "unacceptable."

The QCP would only need to be a 5-10 page document, focusing on:

1. Technical Accuracy Review: How the KTR ensures tools being taught are the current versions used in the field.
2. Section 508 Compliant: Ensuring all digital materials are accessible to users with disabilities (part of the Rehab Act of 1973).

Deliverable

A004 – Quality Control Plan

Performance Standard:

a) Review Cycle: A "30-60-90%" review process where the government approves the design at various stages before full production begins.

The Government shall monitor the Contractor's performance under this contract in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The QASP is a Government-only document and will not be released to the Contractor.

2.9. Performance Evaluation.

Contractor performance is subject to Government surveillance to ensure PWS compliance. The Contractor shall comply with the following:

Access. The Contractor shall permit the CO or authorized representative access to all work records and data used in the performance of the contracted services. The Contractor shall provide support, and not interfere with the CO, Contracting Officer's Representatives (CORs), state, federal, and other designated personnel in the performance of their official duties. The Contractor shall provide access as soon as possible, but not to exceed one (1) workday after the request.

Non-conformance. The Contractor shall identify root causes of non-conformances and shall control them through analysis, corrective actions, and preventive actions. The Contractor shall focus on eliminating the cause to prevent reoccurrence. The Contractor shall maintain records of non-conformities and actions taken. The Contractor shall correct and provide responses to all Government-identified non-conformances in accordance with (IAW) time frames specified by the CO. There are two types of non-conformances: Minor and Major.

Minor Non-conformance. A Minor Non-conformance is a non-conformance, which by itself does not adversely impact mission, safety of personnel and equipment, performance (quality), schedule (delivery), or cost. A Minor Non-conformance does not normally increase risk to the Government. Minor Non-conformances are typically low risk and are communicated through a Corrective Action Request (CAR) notice. First notices are issued for any identified non-conformance, second notices are issued for repeat non-conformances or failing to correct issues within a reasonable amount of time. Upon receipt of a non-conformance notification (first or second notice), the Contractor shall complete applicable sections and return it to the CO within time constraints directed by the CO in the notice. A formal corrective action plan may not be required for minor CAR notices.

Major Non-conformance. A Major Non-conformance is a non-conformance that adversely impacts (or has the potential to impact) mission, safety of personnel and equipment, performance (quality), schedule (delivery), or cost. A Major Non-conformance may also be a significant number of recurring non-conformances, which is an indication of inadequate preventive measures or actions and lowers the Government's confidence that the Contractor can provide quality services on time and within costs. The CO will communicate Major Non-conformances using the CAR notice and will include a suspense date for the Contractor's Corrective Action Plan. As a minimum, the Contractor's Corrective Action Plan shall address:

- Actions taken to fix the immediate problem
- Root cause analysis of the problem to determine cause
- Corrective action on the cause of the problem
- Actions taken to prevent recurrence

2.10. Government Furnished

The Government will make available the materials, communications capability, and information on the dates specified as identified in Attachment 1for use by the Contractor in the performance of this contract.

2.10.1. Government Furnished Property (GFP).

The Government will not provide any GFP for Contractor use on this contract. GFI will be listed on Attachment 1.

2.10.2. Government Furnished Resources.

The Government will not furnish any physical resources.

2.10.3. Government Furnished Information (GFI)

Government staff personnel will be available for technical exchanges with the Contractor. Government personnel will provide technical input, answer questions, review and approve completed work, and provide feedback regarding Contractor efforts. The COR is the primary source of technical guidance for this PWS.

All GFI in contractor possession, regardless of how received, is subject to DFARS 52.227-7025 Limitations on the use or disclosure of government-furnished information marked with restrictive legends. GFI will be listed on Attachment 1.

2.10.4. Materials and Other Direct Costs (ODC)

ODC includes material and licensing support of Delta 1 for the execution and curriculum development and maintenance of CGC. Additional ODCs may occur in performance of contract and are to be reviewed by the COR prior to them being incurred to have government payment. All open market materials and licenses purchases must be approved in advance by the COR. Contractor shall submit invoices for these purchases and provide records to the COR.

For material purchases exceeding $10,000, the Contractor shall obtain review and concurrence, from both the COR and the CO prior to purchase. In addition, the Contractor shall provide at least three quotes to the COR and the CO for determination of reasonable cost and best technically acceptable offeror that meets the Government need. If the contractor recommends a solution other than the lowest cost, detailed rationale shall be provided to the Government. The Contractor shall not break up purchases to meet this threshold. All receipts for charges on the ODC CLIN shall be submitted with the invoice when billed.

3. Performance Requirements

The following section specifies the Performance Objectives and Performance Elements for the contract. Acceptable Quality Level (AQL) is a tolerable variation in the execution of a PWS Standard.

The Contractor shall provide required tools, materials, and labor necessary to support and execute the in-residence courses required by CGC. Technical efforts required by this contract include the maintenance and instruction of in-residence covering key CGC discipline subject matter areas utilizing the ISD Process.

Performance Standard:

Upon mutual agreement between the Government and the Contractor on the finalized CGC Curriculum Development Guide (CDG) and IAW DAFH36-2675, supplied by the Government, to support execution of CGC, the following performance standards will be implemented.

a) Standard: Course iteration will utilize the ISD process and guidance as specified within the CGC Curriculum Development Guide (CDG) and DAFH36-2675.

b) Standard: Contractor course lessons and instructor guides will be developed IAW CGC CDG and DAFH36-2675. These lessons are developed in accordance with the Master List of Objectives for the CGC. See Attachments 2 -5.

Deliverable

A001 – Monthly CGC Status Report. All associated contract performance requirements are to be included in the monthly status report. During the curriculum development the report will include progress updates to the projected development schedule and course documentation. During the piloting stage, the report will include changes made or not made based on feedback of the content.

3.1. Transition

The Contractor shall follow the transition plan submitted as part of the proposal and keep the Government fully informed of status throughout the transition period. Throughout the phase-in/phase-out periods, it is essential that attention be given to minimize interruptions or delays to work in progress that would impact the mission. The Contractor must plan for the transfer of work control, delineating the method for processing and assigning tasks during the phase-in/phase-out periods.

3.2. Associate Contractor Agreements (ACA) RESERVED

3.3. STARCOM Directed Meetings/Events

Contractor personnel shall attend STARCOM newcomer orientation, all calls, and other major organizational related STARCOM meetings deemed necessary by the STARCOM and/or Delta Commander. NDA's for these meetings shall be used as required.

3.3.1. Kick-Off Meeting

The Contractor shall present a kick-off meeting to describe cost, schedule, and performance requirements within 10 days of performance start. The briefing shall include a description of

deliverables, a schedule/plan for lesson design and development (which will subsequently be included in and updated in the Monthly Status Report), as well as key personnel roles and responsibilities.

Deliverable

A005 – Kick-Off Meeting Slides/Handouts

3.3.2. Program Management Review (PMR) RESERVED

3.3.3. Working Group Tag ups

The Contractor shall participate in working group tag-ups with the Government, to occur no less than twice a month, to demonstrate development progress and ensure stylistic and pedagogical cohesion across all course modules. These sessions will serve to verify that independently developed lessons logically stack and integrate into a unified curriculum while adhering to the established delivery schedule. Participation to include comments and recommendations to allow CGC to successfully resolve issues and meet action item suspense's.

3.4. Civilian Guardian Course Descriptions and Requirements

The CGC is structured to guide new Civilian Guardians into becoming fully integrated, space-minded, warfighting Guardians. The CGC begins by establishing a foundational space-minded perspective, requiring graduates to analyze the strategic environment to understand the 'why' behind the USSF mission. From there, it builds towards forging the Guardian identity by examining how USSF doctrine and Guardian warfighting ethos define their unique role and responsibilities and shape their impact as a civilian Guardian. The course then advances from theory to application, challenging students to apply concepts to solve complex, simulated operational challenges. By the conclusion of the course, each Guardian will have constructed a personalized development plan. This final step transforms the course from a singular training event into the starting point of a career-long journey, directly linking personal growth to USSF strategic needs and serving as a powerful tool for talent retention.

The Contractor shall provide all personnel necessary to develop the curriculum which will consist of a blended learning model, beginning with an online portion that is a mix of asynchronous and synchronous online engagements and ending with a one week, immersive in-person engagement.

Contractor developers operate as subject matter experts (SMEs) in space knowledge (as detailed in Attachment 2) and play a critical role in courseware development, validation, maintenance, and instruction. They possess a deep understanding of the subject or tradecraft that will ultimately be covered by the curriculum, and as such, they are considered the definitive expert in this regard. In the course design process, they coordinate with the CGC Gov team in validating the accuracy and relevancy of course scope and sequence, learning outcomes, samples of behavior, learning experiences instructional media, technology integration, mission planning scenarios, and desired levels of learning. These personnel will advise the Government on any course changes or modification.

The contractor's responsibility is to build lessons and activities that teach and assess at the Enabling Learning Objective (ELO) level, with the understanding that successful completion of all ELOs will result in the achievement of the Terminal Learning Objective (TLO).

Performance Standard:

Upon mutual agreement between the Government and the Contractor on the finalized CGC Curriculum Development Guide (CDG) and IAW DAFH36-2675, supplied by the Government, to support execution of CGC, the following performance standards will be implemented.

a) Standard: Course iteration will utilize the ISD process and guidance as specified within the CGC Curriculum Development Guide (CDG) and DAFH36-2675.

b) Standard: Contractor course lessons and instructor guides will be developed IAW CGC CDG and DAFH36-2675. These lessons are developed in accordance with the Master List of Objectives for the CGC. See Attachments 2 -5.

Online Foundation: The online foundation (Modules 0, 1, 2, and 3) is a 40-hour mix of asynchronous and of synchronous. It is designed to provide students with the foundational knowledge required for advanced application. During this phase, students will analyze the strategic space environment, learn core USSF doctrine, and use digital tools like AI to collaboratively produce analytical products. This phase culminates in each student developing a complete first draft of their 18-month career development plan, ensuring they arrive at the residential portion fully prepared to move from theory to practice.

In-Person Application: The in-person application is a culminating, final synthesis and extension of all learning experiences executed over a one-week residential capstone. The goal is to forge foundational knowledge from online learning into practical professional skills. Through high-fidelity simulations, structured peer feedback sessions, and direct engagement with senior leaders and site visits to strategic partners, students practice collaborative problem-solving and decision-making in a facilitated gamified environment. The week's activities also include refining the career development plan and rehearsing the communication strategies needed to advocate for it. This phase is not job-specific qualification training; it is designed to build the core competencies and professional network required of an effective, integrated Civilian Guardian.

Proficiency Level: Learning objectives are written using Bloom’s taxonomy and curriculum, in general, should be developed to achieve proficiency at that level. See Attachment 2.

The Four Knowledge Areas & Capstone of the CGC

The CGC consists of four knowledge areas. Responsibility for developing content in a specific knowledge area is outlined Attachments 2 – 4.

- Knowledge Area 1: The Strategic Environment: Understanding the Battlespace. (Focus: The "Where" and the "How/Why"): The objective of this domain is to establish a foundational space-minded perspective for all participants. The curriculum shall provide instruction on the character of the space domain. Required topics must include its physical nature, the

geopolitical landscape (to include threats and opportunities) of key international and commercial actors, and the governing policies that define it as a contested and congested warfighting domain. Students will also receive the foundational knowledge necessary to build space-mindedness in cyber, intelligence, acquisitions, and space operations. Other key topics include building an understanding of the Space Warfighting organizational architecture across the USSF and Department of War.

- Knowledge Area 2: Doctrinal and Professional Foundations. The Guardian's Identity: Finding Your Place on the Team. (Focus: The "Who" and "My Why"): The objective of this domain is to familiarize students with foundational USSF doctrine, with specific emphasis on "Spacepower," and the professional ethos described in the Guardian Commitment. The curriculum must ensure each civilian can articulate how these foundational principles define their roles and responsibilities within the integrated military and civilian total force structure. Students will be introduced to what it means to be a digital service and how to ethically and agilely employ Artificial Intelligence (AI) and other emerging technologies to enhance effectiveness and efficiency safely in their daily roles and responsibilities.

- Knowledge Area 3: Career Architecture and Strategy: Launching Your Guardian Career. (Focus: The Future): Instruction will be provided on the principles of long-term career planning. Required topics shall include strategies for continuous professional growth, effective mentorship, and professional self-advocacy within the context of the Department of the Air Force.

- Knowledge Area 4: Applied Operational Concepts: From Theory to Decision. (Focus: Application and Synthesis): The course must include a practical application component, requiring participants to engage in a high-fidelity, simulated operational challenge. In this environment, students shall be required to apply doctrinal concepts and demonstrate effective teamwork skills to analyze a complex problem and present viable courses of action.

- Capstone: Successful completion of the course is contingent upon the development, submission, and briefing of a capstone project. The capstone project shall consist of a personalized, space-minded career development plan. This plan must serve as an actionable roadmap that synthesizes concepts from all four learning domains. The primary requirement of the plan is to detail a viable strategy for the individual to enhance their skills and knowledge, with the expressed goal of transforming their specific function into a source of decisive advantage for the U.S. Space Force. See attached Attachments 2 – 5.

3.4.1. The Contractor shall design, develop, and sustain all course materials—including lesson plans, instructional aids, student/instructor guides, and associated assets—throughout the period of performance Working Group Tag ups

All curriculum planning, design, development, and evaluation shall be executed in compliance with industry-standard Instructional Systems Design (ISD) principles, referencing guidance such as DAFH36-2675, AFI 16-1007 and AFH 36-2235 Volumes 1-13.

The Contractor shall reference and draw upon Government-Furnished Information to ensure all developed content is substantively aligned with current Government policy, doctrine, vision, and standards. GFI includes authoritative source doctrine and reference materials (e.g., the strategic and doctrinal publications listed in Attachment 1) that the Contractor shall use to ground and align its content, as well as high-level requirements (TLOs/ELOs) and administrative documents. The Government furnishes no lessons, courseware, or instructional materials built around these references.

The Contractor is responsible for building and iterating on 100% of their assigned curriculum associated with the content identified in Attachments 2 – 5 within the timeline indicated in this PWS, and shall do so using its own pre-existing space subject-matter expertise and personnel; the Government does not furnish, and the Contractor shall not rely on the Government to furnish, subject-matter expertise for the Contractor-assigned technical content. In coordination with the Government to ensure a cohesive course, the Contractor shall develop and maintain a consolidated course syllabus and a Finalized Master List of Objectives. Furthermore, the Contractor shall design and maintain all formative and summative assessment instruments, practical exercises, performance-based rubrics, and materials for in-person simulations. All contractor-developed materials are subject to Government review and approval prior to implementation.

For objectives jointly tagged GOV/KTR in Attachments 2–5, ownership follows the lesson in which the objective is delivered: the party assigned to that lesson authors that instance of the objective. See Attachment 3–4. The Government and Contractor shall collaborate during the design and development stage to ensure all overlapping objectives are cohesive and the curriculum maintains a logical, continuous flow across all modules.

To support continuous improvement, the Contractor shall establish and manage a system to gather student feedback on various stages: individual lessons, whole modules, and final end-of-course.

The initial build-out of the course is the primary deliverable. Subsequent Government-directed updates, as outlined in the Schedule of Deliveries (para 2), shall be accomplished iteratively based on student feedback and andragogical best practices. The Government retains final authority on all course content and instructional methodologies.

Performance Standards

a) Standard: Design and develop materials IAW industry-standard Instructional Systems Design (ISD) and curriculum and materials development principles, referencing guidance such as DAFH36-2675, AFI 16-1007 and AFH 36-2235 Volumes 1-13.

b) Standard: Report updates and questions during Working Group Tag ups and Monthly Status Report

c) Standard: Communicate questions, clarification requests, and any other concerns on the curriculum and material builds

d) Standard: Address questions, clarification requests, and any other concerns from the Government CGC team NLT 2 business days

3.4.2. Course Feedback

The Contractor shall develop the vehicles for gathering student feedback for each section of the course to be used during piloting. The Contractor shall review course critiques during each stage of the pilots and recommend class and/or course changes to the respective CGC leadership.

Performance Standard:

a) Standard: Feedback vehicles will target the full student experience: delivery, pacing, design, content, etc.

b) Standard: During the pilot executions, feedback will be collected after each lesson, module, session, and full pilot execution to ensure both micro and macro views.

c) Standard: Report must include: Overall trend analysis for the module/lesson/session plus any salient student comments. Areas of success for each lesson or session. Issues or areas of concern for each lesson or session. Recommended lesson and/or course changes and a timeline/plan to execute those changes for changes are relevant to their assigned content. The raw feedback data.

d) Standard: Following the full execution of each pilot, a comprehensive report will be complied.

Deliverable

A006 – Post Execution Feedback Analysis

3.4.3. The Contractor shall provide Multimedia support to CGC Government personnel in all necessary multimedia activities used throughout CGC curriculum build. Multimedia support includes the design, development, and production and deployment of multimedia products for use in CGC

The Contractor shall be responsible for the creation of graphics, illustrations, user interfaces, design layouts, and other visual aids using standard software purchased or owned by the contractor (e.g. Adobe Photoshop Creative Suite tools).

The Contractor shall be capable of providing video production support with equipment such as cameras, microphones, lighting, and a green screen. Video must be capable of being delivered across different types of electronic media devices mobile, tablet, and desktop).

The Contractor shall be responsible for licensing agreements in relation to video stock footage, images, and sound sampling.

Performance Standard:

a) Standard: The Contractor shall follow Multimedia Management procedures defined in AFH 36-2235 Vol 5, MIL-HDBK-29612-3A, MIL-HDBK-29612-5 and AFMAN 17-1203.

3.4.4. Courseware Documentation

The Contractor shall provide courseware documentation for all assigned lessons/sessions when finalized and agreed upon by both Government and Contractor. To support the accelerated project timeline, the Contractor shall utilize a rolling delivery model for all courseware documentation. The Contractor shall deliver materials incrementally as soon as the initial build—or subsequent iterative update—for each individual lesson is completed, rather than holding materials for a single, module-wide delivery.

As curriculum design and development is a dynamic process, the Contractor is authorized, and encouraged, to modify previously submitted lessons if subsequent development reveals a need for better cohesion or logical "stacking" across the curriculum. To manage these ongoing updates, the Contractor shall establish and maintain a strict version control system. All submitted courseware, including subsequent revisions to previously delivered lessons or sessions, must be clearly and consistently labeled.

All final files for a given module must be delivered no later than the milestones established in the Schedule of Deliveries (para 2). This ensures the Government has sufficient time for LMS integration, technical configuration, and validation prior to student execution.

Courseware documentation for CGC courses includes (but is not limited to) course syllabi, visual aids (e.g. slides, SCORM materials, photos, videos, templates, etc.), lesson plans (with incorporated instructor guide), assignments (to include instructions, worksheets/templates, grading rubrics, etc.), formative assessments/knowledge checks, course capstone materials, student critique forms, and handouts.

IAW the ISD process, all material will be kept current and relevant throughout the period of performance. Lesson material will be updated following each stage of pilot iteration based on feedback and adult learning practices.

Performance Standard:

a) Standard: The curriculum build out and support shall be IAW ISD principles as stated in AFI 16-1007, AFH 36-2235 Volumes 1-13, DAFH36-2675, and 319 CTS Curriculum Development Guide.

b) The Contractor shall provide support for:

- Curriculum development, to include student facing and instructor facing content
- Courseware management including courseware analysis, design, development, implementation, and evaluation

Deliverable

A007 – Courseware Documentation

4. Applicable Publications

The Contractor shall comply with all documents listed below in the table of publications and referenced under paragraph 3.0, Performance Requirements. The Directive/Guidance (D/G) column indicates the extent of Contractor compliance with the publication that is prescribed by the PWS. A "D" in the column means the publication is a "directive publication," that requires mandatory compliance by the Contractor. A "G" in the column means the publication is a "guidance publication." Compliance with documents listed as guidance is the Contractors' option. If there is any conflict between the directive referenced in PWS paragraph 3.0 and the reference listed in the tables below, the reference in PWS paragraphs 3.0 takes precedence.

When directive chapters, paragraphs, appendices, attachments, etc. are referenced as a standard in this PWS, the standard shall be inclusive of all subordinate paragraphs unless specifically excluded. For example, if the PWS standard lists paragraph 1.2 as directive, and paragraph 1.2 has subparagraphs 1.2.1, and 1.2.2 those subparagraphs are directive as well.

Publications			
D/G	**Pub Number**	**Title**	**Date**
D	AFI 10-701	Operations Security	09 Jun 2020
D	AFI 16-201	AF Foreign Disclosure & Technology Transfer Program	02 Jun 2015
D	AFI 16-1404	Information Security Program Management	29 Jul 2019
D	AFI 17-100	AF IT Service Management	24 Oct 2017
D	AFI 31-501	Personnel Security Program Management	29 Nov 2012
D	AFMAN 17-1302-O	Communications Security Operations (COMSEC)	16 May 2018
D	AFMAN 33-152	User Responsibilities & Guidance for Information Systems	01 Jun 2012
D	AFPD 17.1	Information Dominance, Governance & Management	12 Apr 2016
D	AFSSI 7700	Emissions Security	21 May 2019
D	CJCSI 3213.01D	Joint OPSEC	7 May 2012

D	DFARS 252.227-7032	Rights in technical Data & Computer Software	28 Jun 1995
D	DFARS 252.237-7023	Continuation of Essential Services	Oct 2010 24
D	DoDI 5200.48	Controlled Unclassified Information	Feb 2012
D	DoDI 5205.11	Management, Administration & Oversight of SAPCO	04 Feb 2020
D	DoDI 8140.01	Cyberspace Workforce Management	11 Aug 2015
D	DoDI 8510.01	Risk Management Framework	12 Mar 2014
D	DoDI 8570.01	Commercial/Industry IA Certifications	10 Nov 2015
D	DoDM 5205.07v1	General Procedures	30 Sep 2020
D	DoDM 5205.07v2	Personnel Security	30 Sep 2020
D	DoDD 5205.02E	DoD Operations Security (OPSEC) Program	20 Jun 2012
D	319 CTS CDG	319 CTS Curriculum Development Guide	31 Jan 2024
D	CGC CDG	CGC Curriculum Development Guide	TBD
D	DAFH36-2675	Information for Designers of Instructional Systems	15 April 2022
G	319 CTS OI 36-2203	319 CTS Operations	17 June 2024
G	319 CTS 60-2401	319TH & 42D Standardization and Evaluations Guide	4 Mar 2024

5. Deliverables

The Contractor shall provide deliverables as described in the PWS. Format and delivery schedule for deliverables shall be outlined in the table below All Deliverable distribution shall be by an electronic method unless otherwise specified. Email documents in a Microsoft Office or Adobe Acrobat-compatible format. Submit drawings in a uniform electronic format. Relevant interactive courseware pieces shall be delivered in the specific SCORM-compliant format in which it was developed to ensure full functionality within the Government-provided Learning Management System (LMS). Files exceeding standard email capacity shall be delivered via DoD SAFE or an alternative secure method coordinated with the Government.

Informal, recurring work products may not require a deliverable. These products are still required as described in paragraph 3 of the PWS.

If there is any conflict between the Deliverable reference in paragraph 3 of this PWS and the Deliverable specifics in the following table, paragraph 3 takes precedence. Days referenced shall be calendar days, unless otherwise noted. For recurring Deliverables, if the due date falls on a holiday or a weekend the Deliverable may be sent on the following business day. Contractor format is acceptable, unless a specific format is identified. The Contractor shall not include its name or any logos on any Deliverable except when a Contractor signatory is required by the Deliverable. The Contractor shall ensure all markings included in Deliverables are consistent with the contract's requirements, to include copyright and proprietary markings addressed in the contract's clauses.

Deliverable Table

Identifier	Name	PWS #	Schedule	Distribution
A001	Monthly Status Report (MSR)	2.2	Monthly, NLT 15th of the month after performance	COR PCO
Description: (Contractor format acceptable) As a minimum, the MSR shall detail: - Executive summary detailing a self-assessment of the Contractor's performance during the reporting period to include: - Major tasks/activity status and timeline updates - Contractual issues or risks requiring Government resolution/mitigation - Self-identified performance efforts exceeding the PWS requirements, along with how these efforts provide a benefit to the Government - Self-identified performance deficiencies during the period; including the cause of each identified deficiency, corrective actions, the impact, and actions taken to preclude recurrence - Deliverables submitted - If Deliverables will contain CUI data, ensure this is noted in the description and instruct the Contractor to mark/disseminate/protect IAW CUI regulations				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
A002	Contractor Personnel Roster	2.2.4	At contract award and with any updates or changes.	COR PCO
Description: (Contractor format acceptable) As a minimum, the Roster shall detail: - Roster of all current personnel - Status of their NDA completion (PWS 2.6.6) - Role and area of expertise				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
A003	Non-Disclosure Agreements (NDAs)	2.6.6	Initial: NLT 15 days after contract start. Ongoing: Prior to new personnel starting.	COR PCO

Description:
Signed and verified/certified Government NDAs for all personnel working on the CGC.

Identifier	Name	PWS #	Schedule	Distribution
A004	Quality Control Plan (QCP)	2.8.3	Within 30 days of award	COR PCO

Description: (Contractor format acceptable)
As a minimum, the QCP shall detail:

- How the Contractor shall maintain an inspection system acceptable to the Government covering the services under this contract to include deliverable requirements.
- The Contractor's documented processes and procedures to monitor and control objectives for Services Summary Items, subcontractor relationships, contractor and subcontractor invoicing, and non-conformances.

Identifier	Name	PWS #	Schedule	Distribution
A005	Kickoff Meeting Slides/Handout	3.3.1	NLT 10 days after contract start.	COR PCO

Description: (Contractor format acceptable)
As a minimum, it shall detail:

- A description of deliverables
- A schedule/plan for lesson design and development
- Key personnel roles and responsibilities

Identifier	Name	PWS #	Schedule	Distribution
A006	Post Execution Feedback Analysis (PEFA)	3.4.2	Within two weeks following the execution of each module of the curriculum for both the online and in person portions.	COR PCO

Description: (Contractor format acceptable)
As a minimum, the Feedback Analysis shall detail:

- Overall trend analysis for the module/lesson/session.
- Areas of success for each lesson or session
- Issues or areas of concern for each lesson or session
- Recommended lesson and/or course changes and a timeline/plan to execute those changes for changes are relevant to their assigned content

Following the conclusion of an entire pilot: Overall trend analysis for the course

Identifier	Name	PWS #	Schedule	Distribution
A007	Courseware Documentation	3.4.4	Per lesson/session	COR PCO

Description:

Courseware documentation for CGC courses includes (but is not limited to) course syllabi, visual aids (e.g. slides, SCORM materials, photos, videos, templates, etc.), lesson plans (with incorporated instructor guide), assignments (to include instructions, worksheets/templates, grading rubrics, etc.), formative assessments/knowledge checks, course capstone materials, student critique forms, and handouts.

6. Services Summary

This Services Summary (SS) identifies the major performance objectives and performance thresholds required for Contractor performance. The Government retains the right to inspect, assess and enforce all services required by this contract, regardless of their inclusion in this SS.

SS	Requirement	PWS Para	Threshold
1	Curriculum Development and Iteration – Perform all associated curriculum development and iteration actions as required by Government and 319 CTS OI, CGC CDG, and this PWS.	2.3, 3, 3.3.3, 3.4, 3.4.1, 3.4.2, 3.4.4	Performance is acceptable when: - CGC curriculum is developed and iterated IAW this PWS and remains current and relevant with current USSF and DoD actions and positions. - Technical content is accurate and authored by qualified space SMEs per para 2.3. - IAW the ISD process, all material is kept current and relevant; IAW the CGC CDG, lesson material is updated at regular intervals as specified in this PWS. - ISD support is provided IAW 319 CTS OI 36-2203, the CGC CDG (when finalized and agreed upon by both Government and Contractor), and IAW ISD principles as stated in AFI 16-1007 and AFH 36-2235 Volumes 1-13.
2	Multimedia Support – Creation of graphics and presentations for CGC lessons and mission areas	2.3, 3.4.3	Performance is acceptable when: - Multimedia products (graphics, video, interactive media) are produced IAW AFH 36-2235 Vol 5, MIL-HDBK-29612-3A, MIL-HDBK-29612-5, and AFMAN 17-1203 (per para 3.4.3). - Multimedia, templates, and other products are integrated across all CGC materials,

			maintaining a current, professional, high-quality look and feel.
3	Program Management and Regulatory Compliance – Contract follows all applicable rules, regulations, and laws. PWS requirements are executed on time and are of high quality.	2.3, 3.1, 3.3, 3.3.1	Performance is acceptable when: - Personnel are ready, qualified, and on time for meetings and other needs as described in this PWS. - All deliverables are delivered on time, accurate, and of high quality. - Zero negative personnel actions (e.g., discriminatory or inappropriate behavior) that go uncorrected within an appropriate amount of time. - Zero violations of rules, regulations, and laws applicable to this PWS. - Zero personnel requirement gaps of greater than 30 days, unless coordinated with the Government in advance.

Attachment 1 – Government Furnished Information

Government Furnished Information
CGC TLOs, ELOs, and Guiding Questions
Relevant Public Facing GOV Materials: Objective Force 2040, Environment 2040, USSF 101, SFDD1-1, Guardian Spirit Handbook, CSO's C-Notes

Attachment 2 – Tentative CGC Objectives

The provided list of objectives is tentative and may be refined during the design phase upon mutual agreement between Government and Contractor, provided changes remain within the original scope of work.

In areas of shared responsibility for an objective, Government or Contractor is responsible for the objective as it applies to the lesson it is addressed in. See Attachment 3-4. The Government and Contractor shall collaborate during the design and development stage to ensure all overlapping objectives are cohesive and the curriculum maintains a logical, continuous flow across all modules.

The first digit of a Terminal Learning Objective (TLO) or Enabling Learning Objective (ELO) corresponds to the specific knowledge area it supports (e.g., all TLOs/ELOs that begin with "1" fall under Knowledge Area 1: Understanding the Battlespace).

Course Learning Objectives (CLOs)

- The Strategic Environment
  - CLO 1 Analyze the strategic space environment, including its physical nature, key actors, governing policies, and prevalent threats, to establish a foundational space-minded perspective.
- Doctrinal & Professional Foundations
  - CLO 2 Articulate how foundational USSF doctrine, the Guardian professional ethos, and core ethical principles define the distinct and complementary roles, responsibilities, and expected conduct of a civilian Guardian within the O/E/C team.
- Career Architecture & Strategy
  - CLO 3 Construct a personalized 18-month career development plan that includes specific, actionable goals for professional growth, mentorship, and continuous learning and apply foundational communication strategies to advocate for professional development aligned with the strategic needs of the Space Force.
- Applied Operational Concepts
  - CLO 4 Apply USSF doctrinal concepts, collaborative teamwork skills, and a structured problem-solving framework to analyze a simulated, complex operational challenge and present a justified course of action.

Terminal and Enabling Learning Objectives

KTR = Contractor / GOV = Government

#	Objectives	Guiding Question	Assigned To:
1.1	Describe the physical characteristics and operational considerations of the primary		KTR

	orbital regimes (LEO, MEO, GEO, HEO).		
1.1.1	Define Low Earth Orbit (LEO), Medium Earth Orbit (MEO), Geostationary Orbit (GEO), and Highly Elliptical Orbit (HEO), including their characteristic altitudes.	What are the four main 'highways' in space where satellites operate?	KTR
1.1.2	Explain the primary use, one advantage, and one disadvantage of each orbital regime.	Why would you choose one orbit over another for a specific mission?	KTR
1.1.3	Match common space missions (e.g., Earth imagery, PNT, strategic missile warning) to their optimal orbital regime.	If you wanted to take pictures of Earth, where would you park your satellite? What about for GPS?	KTR
1.2	Explain how the space domain is both congested (space debris) and contested (adversary threats).		KTR
1.2.1	Define the term "space debris" and identify its primary sources.	What is "space junk," and why is it one of the biggest threats to satellites?	KTR
1.2.2	Explain the concept of Kessler Syndrome and its potential impact on space operations.	What happens if too much debris accumulates in orbit?	KTR
1.2.3	Define the term "contested domain" in the context of space and provide an example of an activity that demonstrates the contested nature of space.	What does it mean when we say space is a "contested domain"? What makes it a potential battlefield?	KTR
1.3	Identify the core tenets of foundational U.S. space history, policy, and law.		KTR
1.3.1	Describe the key historical milestones and strategic imperatives that led to the	Why does the Space Force even exist? What key events and growing threats made the	KTR

	establishment of the U.S. Space Force.	creation of a separate service a national security necessity?	
1.3.2	List the key principles of the Outer Space Treaty of 1967 (e.g., nonappropriation, peaceful purposes).	What are the fundamental "rules of the road" for all nations in space?	KTR
1.3.3	Identify the primary goals related to space in the current National Security Strategy.	What does U.S. national strategy say about why space is critical for security?	KTR
1.3.4	Differentiate between the concepts of "militarization" and "weaponization" of space.	What is the critical difference between using space for military purposes and placing weapons in space?	KTR
1.4	Analyze the spectrum of counterspace threats by categorizing adversary actions into the "5 Ds" and evaluating their potential impact on mission assurance.		KTR
1.4.1	Define each of the "5 Ds" of counterspace (Deception, Disruption, Denial, Degradation, and Destruction) and provide a common example of each.	What are the main ways an adversary can actually interfere with our satellites?	KTR
1.4.2	Differentiate between kinetic and non-kinetic effects, explaining the strategic implications of each (e.g., debris generation vs. reversibility).	What is the difference between a 'hard kill' and a 'soft kill,' and why does the Space Force care more about the long-term debris of a kinetic attack than the temporary disruption of a non-kinetic one? Why might an adversary choose to temporarily blind a satellite with a laser instead of destroying it with a missile, and how do the long-term consequences of that choice (like space debris) alter the strategic landscape for everyone?	KTR

1.4.3	Categorize counterspace capabilities using the "5 Ds" framework and provide a rationale for each categorization.	Given a real-world scenario, can you identify the specific type of threat being used and explain why it fits into that category?	KTR
1.4.4	Analyze a notional adversary action to determine the correct "D" category and assess its potential impact on a specific joint warfighting mission.	When an adversary attacks a satellite, what is the actual, on-the-ground impact to the warfighter who relies on it?	KTR
1.5	Analyze the critical interdependencies between space and cyber operations to determine how non-kinetic vulnerabilities in the ground, link, or space segments can degrade or deny strategic capabilities.		KTR
1.5.1	Examine the three segments of a space system (ground, link, space) to identify their specific cyber vulnerabilities and access points.	If a hacker wants to take down a multi-billion-dollar satellite, why might they never actually target the spacecraft itself? If our satellites remain physically untouched but the mission fails, where was the 'kill chain' likely broken, and why is the ground segment often our weakest link?	KTR
1.5.2	Analyze how a localized cyberattack on a specific segment (e.g., a ground station) cascades to impact the overall space capability and supported joint forces.	How can a tiny hack on the ground lead to a complete loss of capability in orbit? How does a single broken link impact the whole joint team?	KTR
1.5.3	Evaluate a real-world or simulated cyber operation (e.g., the Viasat attack) to determine how it successfully denied, degraded, or disrupted a satellite's function without physical damage.	Looking at real-world events like the 2022 Viasat cyberattack, how exactly does an adversary turn a critical space capability into a 'floating brick' without firing a single weapon?	KTR
1.6	Articulate the difference between Space Domain Awareness (SDA) and space intelligence.		KTR

1.6.1	Define SDA as the "what, where, and when" and space intelligence as the "who, why, and how" (characterization and intent).	What's the difference between knowing what a satellite is doing versus knowing why it's doing it?	KTR
1.6.2	Given a notional scenario, correctly label the information provided as either SDA data or intelligence.	Is tracking a satellite's location an act of awareness or an act of intelligence?	KTR
1.7	Explain how the USSF provides space capabilities and effects to the joint warfighting ecosystem.		GOV
1.7.1	Differentiate between the role of the Space Force (to organize, train, and equip) and a Combatant Command like USSPACECOM (to employ forces).	The Space Force builds the team, but who calls the plays during a conflict? What's the difference between USSF and USSPACECOM?	GOV
1.7.2	Identify the primary USSF mission areas and categorize them under the core functions of Space Control, Global Mission Operations, and Space Access.	What are the "crown jewels"—the core missions—that the USSF provides, and how are they officially organized?	GOV
1.7.3	Differentiate between military power projected 'in,' 'from,' and 'to' space, providing a practical example for each category.	Doctrine says we project power "in, from, and to" space. What does that actually mean in the real world? Can you give a simple example of each type of operation?	GOV
1.7.4	Identify the five primary categories of joint partners (Combatant Commands, Sister Services, Interagency, Allies, Commercial).	Who are the main players on the U.S. space team, and what is each of their primary jobs? Who are the ultimate "customers" and "teammates" of the Space Force? (e.g. NRO, NGA, NASA, NOAA)	GOV
1.7.5	Explain the importance of using "joint language" to translate space capabilities into warfighter effects for different service partners.	Why is it critical for Guardians to speak the language of the Soldier, Sailor, Airman, and Marine?	GOV

1.7.6	For at least three core missions, articulate a specific "warfighter effect"—a tangible benefit to another service member.	How does a GPS satellite actually help a Marine on the ground? Let's connect the dots.	GOV
1.7.7	Describe the distinct roles and missions of the Space Force Field Commands and their Deltas and explain how their missions are interconnected.	How is the Space Force organized to deliver its capabilities? Who are the "Acquirers" (SSC), "Operators" (CFC), and "Trainers" (STARCOM), and how do they work with the Operational Deltas? What is one major trend shaping the Space Force's future growth?	GOV
1.7.8	Describe the basic components of the USSF warfighting architecture, including the roles of Combat Deltas and the purpose of SPAFORGEN.	How is the Space Force operationally structured to fight? What is a Combat Delta and how does the USSF prepare its forces for deployment? What is the difference between a Combat Delta and an Operational Delta?	GOV
1.8	Compare and contrast the primary space capabilities, strategic goals, and operational postures of the United States and key international actors.		KTR
1.8.1	Explain the strategic context behind designating China as a "pacing competitor" and Russia as an "acute threat."	Why do we use different strategic terms for China and Russia, and what does that tell us about how we plan to counter them?	KTR
1.8.2	Compare a specific U.S. space capability (e.g., PNT or SDA) with a similar capability fielded by a primary competitor, highlighting areas of strategic advantage or vulnerability.	When we look at our top capabilities side-by-side with our adversaries, where do we have the high ground, and where are we playing catch-up?	KTR
1.8.3	Explain how the space capabilities of a major U.S. ally integrate with and complement U.S. space	We don't fight alone. How do the specific tools and satellites of our closest allies actually plug	KTR

	operations to achieve a strategic advantage.	into our architecture to make the "one team" stronger? How do our allies help us maintain a strategic advantage in space?	
1.9	Explain the complexities of the global space economy and how variables such as financial investment, human capital, and commercial innovation impact U.S. national security space operations.		KTR
1.9.1	Explain how the commercial space sector and private financial investment drive technological innovation and capability development for the DoD.	How does the business of space—the influx of private money and commercial innovation—actually affect the tools and capabilities the Space Force brings to the fight?	KTR
1.9.2	Describe the impact of human capital challenges (e.g., STEM workforce shortages, specialized talent retention) on the sustainability of the space industrial base.	We can buy satellites, but can we find the people to build and fly them? How does the fierce competition for top-tier talent impact our long-term national security?	KTR
2.1	Articulate how core and foundational USSF doctrine defines the distinct and complementary roles and responsibilities of all Guardians.		GOV
2.1.1	Define "Spacepower" and identify the core USSF functions.	What is "Spacepower," and what are the three main jobs the Space Force does for the nation?	GOV
2.1.2	Differentiate between the general roles and responsibilities of Officers (strategic leadership), Enlisted (technical expertise/mission execution), and Civilians (specialized expertise/continuity) within the USSF.	How do the general roles of Officers, Enlisted, and Civilians differ? What unique value does each bring to the team?	GOV

2.1.3	Explain how a civilian Guardian's specialized expertise contributes to a specific USSF core function, enabling the broader O/E/C team to achieve its mission.	Why do we need all three? How does your specific civilian role act as a "force multiplier," enabling your Officer and Enlisted teammates to succeed in their jobs and accomplish the mission?	GOV
2.2	Analyze the components of the Guardian professional identity by explaining how our Core Values shape our character, how our Guardian Spirit shapes our mindset, and how professional Customs enable our integration.		GOV
2.2.1	Explain the four Guardian Values and how they comprise the Guardian Commitment.	What are the four core values that define a Guardian's character and how do they shape the expectations that the Space Force has of you as a Guardian first and a civilian second? Character: Why is doing the right thing, especially when it's difficult or unpopular, the absolute foundation of military service? Connection: How does prioritizing connection actually make our small service more powerful and agile than a larger bureaucracy? Commitment: What is the difference between simply working a job and demonstrating a commitment to the profession of arms? Courage: Why does a culture of innovation require intellectual courage as much as physical bravery?	GOV
2.2.2	Define the Guardian Spirit in terms of key attributes and expected attitude.	What does the "Guardian Spirit" mean in terms of our expected attitude and mindset? How does it define our responsibility to be Principled Public Servants, Space-minded Warfighters, Bold	GOV

		and Collaborative Problem Solvers?	
2.2.3	Integrate the Guardian Values into a professional framework for navigating daily workplace challenges and team dynamics.	Values aren't just for posters—they are operational tools. When faced with a high-pressure deadline or a conflict with a teammate, how might you actively use these values to determine the right course of action? How do these values collectively shape the way we solve problems as 'one team'?	GOV
2.2.4	Apply an innovation mindset by challenging assumptions and using a "fail fast, fail forward" approach to creatively solve problems.	The Space Force must move faster than its adversaries. How can we practice a "fail fast, fail forward" mindset to rapidly test new ideas and find creative solutions to tough problems, especially when resources are limited?	GOV
2.2.5	Identify basic military customs and courtesies, including rank recognition and forms of address, to foster effective communication with uniformed counterparts.	What are the basic 'rules of the road' for interacting with my uniformed teammates, like how to address them and understand rank, to ensure you feel confident and respectful in your daily work?	GOV
2.3	Apply a framework for ethical decision-making by synthesizing foundational public service principles with Guardian ideals and the unique competencies of a Civilian Guardian.		GOV
2.3.1	Identify the core tenets of public service ethics that provide the foundation for all government employees as defined in the Principles of Ethical Conduct for Government Employees.	What are the foundational ethical rules that apply to all federal employees as our baseline?	GOV

2.3.2	Explain how the Guardian ideals of being a "Principled Public Servant" and a "Bold and Collaborative Problem Solver" shape the USSF's approach to decision-making.	Beyond the basic rules, what does it mean to make decisions like a Guardian? How do we balance the need to be bold with the requirement to be principled? As a subject matter expert, how do you ethically balance providing candid, data-driven advice with supporting a commander's stated intent, especially when you disagree? How is providing your honest, expert opinion a critical component of your ethical duty to the mission and the taxpayer?	GOV
2.3.3	Describe how a Civilian Guardian's unique competencies—such as specialized expertise, organizational continuity, and specific authorities (e.g., obligating funds)—create distinct ethical responsibilities and opportunities for influence.	As a civilian, you have special skills and authorities that your military teammates don't. How do these unique roles change the way you approach your ethical responsibilities and influence decisions? How does providing "organizational continuity" help a unit uphold its ethical obligations over the long term, despite frequent military personnel turnover? When a new leader arrives, how does the senior civilian's "corporate knowledge" serve an ethical function in advising that leader on past challenges and successes? In what way is being a faithful steward of the organization's history and processes an ethical responsibility?	GOV
2.3.4	Given an ethical dilemma, apply a relevant USSF principle or Guardian value to justify a recommended course of action.	When faced with a tough 'gray area' decision, how can you use these principles and values as a compass to guide me to a sound and defensible choice?	GOV

2.4	Explain what it means for the USSF to be a "Digital Service" and how AI and emerging tech can be ethically employed to enhance mission effectiveness.		GOV
2.4.1	Define the "Digital Service" philosophy and identify one way a nontechnical Guardian can contribute to the Digital Service ideal.	What does it really mean to be a "Digital Service," and how does that affect our daily work? How can you contribute to that culture, even if I'm not in a technical role?	GOV
2.4.2	Apply basic prompt engineering techniques to partner with an AI assistant, while evaluating its outputs for accuracy/bias and adhering to security protocols for all inputs.	How do you effectively use an AI assistant as a productivity partner, and what are the critical "Rules of the Road" for using it safely and verifying its work?	GOV / KTR
2.4.3	Utilize an AI assistant as a 'Red Team' partner to critically assess and identify risks or weaknesses in one's own ideas, plans, or proposed solutions.	Beyond getting answers, how can you use AI as a sparring partner to challenge my assumptions and find the hidden flaws in my own ideas before someone else does?	GOV / KTR
2.5	Connect a Civilian Guardian professional role to a specific USSF core mission and a Guardian value.		GOV
2.5.1	Given the USSF core missions and Guardian values, select the ones most aligned with their job series or function.	Which USSF core mission does your job directly support? Which Guardian value resonates most with you?	GOV
2.5.2	Draft a personal statement that links the daily tasks or overall job responsibilities to that core mission and value.	How can you draw a straight line from your daily tasks to the success of a joint warfighter?	GOV
3.1	Identify key strategies, tools, and opportunities required to build a robust career development plan.		GOV

3.1.1	Complete a self-assessment of current skills and future career aspirations to establish an overall career goal.	Where are you now in your career, and where do you want to be in the next 18 months?	GOV
3.1.2	Research and identify accredited developmental opportunities (e.g., DAU courses, Civilian Developmental Education) relevant to career goals using official DAF/USSF resources.	The Air Force and Space Force provide a huge number of programs. Where do you look to find the official, accredited courses and career opportunities that will help me get ahead?	GOV
3.1.3	Employ an AI partner to conduct targeted discovery of non-traditional, unaccredited development opportunities (e.g., commercial certifications, industry networks) that directly support specific career objectives.	The official catalog won't have everything you need. What other resources like certifications, podcasts, or professional groups or organizations can you use to build your expertise? How can you use AI as a strategic research partner to find the resources and opportunities that will actually give you an edge?	GOV
3.1.4	Define the role of a traditional coach and a traditional mentor.	What is the difference between a coach and a mentor?	GOV
3.1.5	Explain the unique benefits of a peer-to-peer mentorship/coaching relationship, such as shared contextual understanding and mutual skill development.	Why might your most valuable mentor be the person sitting next to you? What unique benefits does a peer relationship offer that a senior mentor cannot?	GOV
3.1.6	Describe a strategy for initiating and maintaining a mutually beneficial peer mentorship.	How do you formally ask a peer for a mentorship relationship without making it awkward? What does a good, structured peer relationship look like?	GOV
3.1.7	Identify the actions and preparations you can proactively take as the receiver to maximize the value of any developmental relationship	Whether your mentor is a senior leader or your peer, what are your responsibilities to make the relationship successful and not waste their time? How do you ensure you are not wasting your mentor's time? What proactive steps can you take to drive the	GOV

		relationship forward and get the most out of every interaction?	
3.2	Construct a personalized 18-month career development plan that synthesizes career goals with specific, actionable opportunities for growth.		GOV
3.2.1	Write at least one specific, measurable, achievable, relevant, and time-bound (SMART) goal for professional training, based on the opportunities discovered.	Now that you have a list of potential opportunities, how do you turn that research into a concrete, actionable training goal for your IDP? What specific training can help you get to where you want to be?	GOV
3.2.2	Write at least one SMART goal for networking or relationship-building.	Building a strong professional network is more than just finding mentors; it's about creating your career's support system. Who are the key people—including knowledgeable peers, customers, key stakeholders, and even friendly experts in other offices—that you need to connect with to be more effective in your current job and prepare for your next one? What is one specific action you can take to build that relationship?	GOV
3.2.3	Evaluate the relationship between personal resilience and professional effectiveness in a high-tempo environment, and develop a proactive resilience strategy integrated into a career development plan.	A high-stress job requires a deliberate plan for personal sustainability. How does your personal well-being directly impact your ability to perform the mission effectively? Based on your own self-assessment, what is one specific, actionable goal you will add to your career plan to proactively manage stress and build your long-term resilience?	GOV

3.2.4	Populate a draft career plan template with the developed goals, tools, and opportunities.	How do you organize all of your research and goals into a first draft of your professional career plan?	GOV
3.2.5	In a peer review session, share the draft career plan to gather feedback and discover new opportunities and strategies from classmates.	Your peers are one of your greatest resources. How can you leverage their diverse experiences and perspectives to find new opportunities and identify blind spots in your own career plan?	GOV
3.2.6	Refine the final career plan by synthesizing self-assessment, research, and peer feedback into a cohesive, actionable document.	Now that you have conducted research and received feedback, what ideas, information, and advice will you incorporate? How do you bring all of this together into a polished career plan?	GOV
3.2.7	Identify at least one immediate, actionable step to take in the month following the course to begin executing the career plan.	Your plan is written. Now what? What is the very first concrete step you will take when you get back to your desk to ensure this plan doesn't just sit on a shelf?	GOV
3.3	Draft a professional introductory message to a potential mentor.		GOV
3.3.1	Identify two qualities or experiences desired in a potential mentor.	What are you looking for in a mentor?	GOV
3.3.2	Using a template, draft a professional introductory message that states your purpose, briefly outlines your goals, and respectfully requests a short introductory meeting.	How do you write a professional email to a senior leader asking for mentorship without sounding demanding?	GOV
3.4	Apply effective communication and advocacy strategies to articulate professional development needs and civilian-specific career		GOV

	considerations to military and civilian supervisors.		
3.4.1	Identify key differences between the military and civilian personnel systems, including performance management, awards, and developmental paths.	Military supervisors and bosses operate under a completely different career system. What are the key differences you need to understand to avoid confusion and effectively manage your own career?	GOV
3.4.2	Demonstrate the ability to advocate for personal professional development by articulating how a specific developmental opportunity or career goal directly enhances team capabilities and supports the strategic intent of the USSF.	How do you prepare for a career conversation with your supervisor to ensure it's productive and professional? Your supervisor is busy and budgets are tight. How could you frame your request for a certification course or time for personal professional development not as something you want, but as something that will benefit the team? What should your talking points be? How do you translate the benefit to the mission?	GOV
4.1	Apply a simplified planning framework to analyze a complex, simulated operational challenge and develop viable courses of action.		KTR
4.1.1	List the steps of the provided problem-solving framework.	When faced with a crisis, what is a simple, structured way to analyze the problem?	KTR
4.1.2	Differentiate between verified facts and operational assumptions within a complex scenario, and analyze how unverified assumptions increase mission risk.	When the pressure is on, how do you separate what you actually know from what you are merely guessing, and why is a bad assumption the fastest path to failure?	KTR

4.1.3	Formulate a concise problem statement that identifies the core challenge in the scenario.	How do you boil down a complicated scenario into a clear, simple problem statement?	KTR
4.1.4	Brainstorm and build out at least two distinct and viable Courses of Action (COAs) to address an identified problem.	When faced with a challenge—from a budget shortfall to an on-orbit threat—how do you develop multiple, distinct options instead of just getting stuck on the first idea you have?	KTR
4.1.5	Identify the key operational considerations for each COA, including required resources, potential mission risks, and the role of internal or external partners.	A good idea isn't a plan until you know what it 'costs.' For each option, what do we need, what could go wrong, and who do you need to partner with? What assumptions did you make when building out your COAs?	KTR
4.2	Justify and defend a strategic recommendation by articulating how the chosen course of action optimizes mission outcomes within the framework of USSF doctrine, goals, and values.		KTR
4.2.1	Identify the potential weaknesses, friction points, and unintended consequences in a proposed Course of Action.	Before you fall in love with your own plan, what is the strongest argument against it? What are the hidden flaws or risks that could cause this plan to fail? Who could you talk to, or what tools/resources could you use to help you "red team" your variables and fact-check your assumptions and data?	KTR
4.2.2	Summarize the strategic merits and required trade-offs of at least two distinct COAs to provide leadership with an objective view of the options.	Leadership rarely has an easy choice. How do you present two different strategies so decision-makers understand exactly what they are gaining and what they are giving up for each?	KTR
4.2.3	Explain the rationale for a recommended COA, referencing	When leadership asks 'Why this one?', how do you defend your	KTR

	Guardian Values and USSF doctrine to justify the chosen balance of risk and reward.	choice by proving it is the most ethically and doctrinally sound path forward for the Space Force?	
4.3	Explain how an external partner's capability could have influenced a simulated scenario.		KTR / GOV
4.3.1	Identify a key moment or decision point in the simulated scenario.	In our simulation, was there a point where more information would have changed everything?	KTR / GOV
4.3.2	Select one external partner (e.g., a commercial satellite imagery company, an allied nation's SIGINT system).	Which of our partners could have helped at that key moment?	KTR / GOV
4.3.3	Explain how a specific capability from that partner could have provided a tactical advantage or altered the outcome at that key moment.	Why is the "Partner to Win" concept not just a slogan, but a strategic necessity?	KTR / GOV
4.4	Synthesize insights from a partner site visit and a senior leader engagement to explain how the "one team" ecosystem (including joint, interagency, allied, and commercial partners) enables the USSF mission.		GOV
4.4.1	During a strategic partner engagement, identify at least one specific capability or process that directly contributes to or could be leveraged for a USSF mission area.	As you tour this facility, look past the specific technology. Find a "tool"—one key capability or process—and ask yourself: How could (or how does) this specific thing help the Space Force accomplish one of its core missions?	GOV
4.4.2	During a senior leader engagement, identify at least one key strategic challenge or priority that requires a	As you listen to this senior leader, don't just listen to their career story. Listen for the problems they are trying to solve. What are the challenges	GOV

	collaborative, "one team" approach to solve.	they are facing that the Space Force cannot solve alone? Also, listen for how they talk about the people needed to solve those problems.	
4.4.3	In a culminating debrief, articulate how the specific partner capability (from the site visit) could be used to help address the strategic challenge (identified by the senior leader).	Connect the dots. How can the specific tool or process we saw on our site visit be used as part of the solution to the big problem our senior leader described?	GOV / KTR

Understanding the TLO and ELO Structure

To ensure precise curriculum development for the Civilian Guardian Course, it is important to understand the relationship between Terminal Learning Objectives (TLOs) and Enabling Learning Objectives (ELOs) as used in the course design. The contractor's responsibility is to build lessons and activities that teach and assess primarily at the ELO level, with the understanding that successful completion of all ELOs will result in the achievement of the TLO.

- A TLO is a high-level statement that describes a broad competency a student will possess upon course completion. It represents a complete, major capability we are building. For example, TLO 3.1, "Apply a simplified planning framework...," describes the overall skill of using a problem-solving model.

- An ELO is a smaller, discrete, and measurable learning step that contributes to achieving the TLO. The ELOs are the specific building blocks of knowledge and skill that, when combined, allow the student to accomplish the TLO.

On Overlapping Language: Occasionally, there will be an ELO that uses language very similar to its parent TLO. is intentional and occurs when a single ELO represents the primary action, culmination of a learning sequence, and/or a building block for an even larger, more complex synthesis later on. The TLO serves as the "umbrella" competency, and the ELOs are the specific, sequential steps required to demonstrate that competency.

Attachment 3 – CGC Tentative Sequencing & Pacing for Online Modules

The provided sequence and pacing is tentative and may be refined during the design phase upon mutual agreement between Government and Contractor, provided changes remain within the original scope of work.

Responsibility for the development of individual Modules and Lessons is based on the TLOs and ELOs of that module, lesson, or day.

Module / Lesson Title	Associated Objectives	Summary	Delivery	Est. Time
Pre-Course: Welcome & Onboarding	GOV	**Summary:** Administrative orientation, syllabus review, and cohort network activation.	Async + Sync	1 Hours
Module 0: Guardian AI Partnership	2.4, 2.4.1, 2.4.2	**Summary:** Introduces the "Digital Service" philosophy, AI security protocols (OPSEC/CUI boundaries), and basic prompt engineering.	Async	3 Hours
Module 1, Lesson 1.1: The Strategic Arena	1.1, 1.2, 1.1.1-1.1.3, 1.2.1-1.2.3	**Summary:** Explores the physical characteristics of space, orbital regimes, and the concepts of a congested and contested domain.	Async	3.5 Hours
Module 1, Lesson 1.2: The Rules of the Game	1.3, 1.4, 1.3.1-1.3.4, 1.4.1-1.4.4	**Summary:** Covers foundational U.S. space history, international policy, and introduces the "5 Ds" counterspace threat framework.	Async	3.5 Hours
Module 1, Lesson 1.3: Modern Threats & Key Concepts	1.5, 1.6, 1.5.1-1.5.3, 1.6.1-1.6.2	**Summary:** Analyzes the cyber interdependencies of space systems and articulates the difference between Space Domain Awareness (SDA) and Intelligence.	Async	3.5 Hours
Module 1, Lesson 1.4: The Joint Ecosystem & Dossier	1.7, 1.8, 1.9, 1.7.1-1.7.8, 1.8.1-1.8.3, 1.9.1-1.9.2	**Summary:** Maps the joint warfighting ecosystem, global actors, and the impact of the space economy/industrial base.	Async + Sync	4.5 Hours
Module 2, Lesson 2.1: The Guardian Identity	2.1, 2.2, 2.1.1-2.1.3, 2.2.1-2.2.5, 2.4.3	**Summary:** Defines O/E/C roles, the Guardian Spirit, military customs, and the application of an innovation mindset.	Async	5.0 Hours

Module 2, Lesson 2.2: The Guardian's Purpose	2.3, 2.5, 2.3.1-2.3.4, 2.5.1-2.5.2	**Summary:** Applies ethical decision-making frameworks to the unique competencies of Civilian Guardians.	Async + Sync	5.0 Hours
Module 3, Lesson 3.1: The Career Plan (Part 1 - Creation)	3.1, 3.2, 3.1.1-3.1.7, 3.2.1-3.2.4	**Summary:** Teaches career self-assessment, discovery of accredited/unaccredited opportunities via the "Resource Safari," and writing goals for the IDP.	Async + Sync	8 Hours
Module 3, Lesson 3.2: Mentorship & Final Prep	3.3, 3.4, 3.3.1-3.3.2, 3.4.1	**Summary:** Differentiates military vs. civilian systems and provides strategies for initiating peer and senior mentorship.	Async	3 Hours
		ONLINE TOTAL:		40 Hours

Attachment 4 – CGC Tentative Sequencing & Pacing for Capstone Portion

The provided sequence and pacing is tentative and may be refined during the design phase upon mutual agreement between Government and Contractor, provided changes remain within the original scope of work.

Areas of responsibility and duration are denoted next to each session.

Each day accounts for around 6 hours of programmed instructional content and activities. The remaining time is reserved for Government-managed administrative housekeeping, breaks, etc..

Day 1: Introductions, Identity, & Ethics

- Session 1: Course Kick-off & Senior Leader Engagement (GOV, 1.5 hours)
  - Summary: Introductions, cohort activation, and opening remarks outlining strategic challenges.
  - Assesses: ELO 4.4.2
- Session 2: The Innovation Showcase (GOV, 1.5 hours)
  - Summary: Debriefing the online digital prototypes and AI Red Team failures.
  - Assesses: ELOs 2.2.4, 2.4.3
- Session 3: Doctrinal Synthesis (KTR, 1.5 hour)
  - Summary: Connecting foundational doctrine to modern space threats.
  - Assesses: Synthesis of Modules 1
- Session 4: Doctrinal Synthesis (GOV, 1.5 hour)
  - Summary: Connecting foundational doctrine to modern space threats.
  - Assesses: Synthesis of Module 2 + Dilemma discussion on ethical frameworks and decision making under organizational pressure.

Day 2: Career Alignment & Tabletop 1

- Session 1: IDP Peer Review Clinic (GOV, 1.5 hours)
  - Summary: Rapid, structured peer review to identify blind spots in online-drafted career plans.
  - Assesses: ELO 3.2.5
- Session 2: Planning Framework Intro (KTR & GOV, 1.0 hour)
  - Summary: Introducing the simplified planning model for complex problem-solving.
  - Assesses: ELOs 4.1.1, 4.1.2, 4.1.3
- Session 3: The Scaffolding Simulation (KTR & GOV, 3.5 hours)
  - Summary: A rules-based tabletop wargame testing the planning framework.
  - Assesses: ELOs 4.1.4, 4.1.5, TLO 1.8

Day 3: Strategic Engagement ("Partner to Win")

- Session 1: Partnership Fundamentals (KTR & GOV, 1.5 hours)
  - Summary: Pre-brief on joint, interagency, and commercial partnering expectations.
- Session 2: SME / Additional Leader Engagement (GOV, 1.5 hours)
  - Summary: Follow-on briefing to discuss specific problems and how the USSF

partners to solve them. Also, to provide the “warfighter perspective.”
    - Assesses: ELO 4.4.2
- Session 3: Industry Day / Partner Site Visit (GOV, 4.0 hours)
    - Summary: Extended on-site tour/engagement to identify external capabilities.
    - Assesses: ELO 4.4.1

Day 4: Dynamic Problem Solving (Tabletop 2)

- Session 1: Strategic Synthesis Debrief (GOV, 1.0 hour)
    - Summary: Facilitated discussion connecting the "Tool" to the "Problem."
    - Assesses: ELO 4.4.3 (Articulate how tool addresses problem).
- Session 2: Dynamic Simulation Execution (KTR, 3.0 hours)
    - Summary: A narrative-driven crisis scenario with timed friction injects. Teams adapt COAs.
    - Assesses: ELO 4.2.1
- Session 3: Simulation Conclusion & AAR (KTR, 2.0 hours)
    - Summary: Finalizing COAs and briefing leadership on trade-offs.
    - Assesses: ELOs 4.2.2, 4.2.3, TLO 4.3

Day 5: Career Capstone & Synthesis

- Session 1: Career Advocacy (GOV, 1.5 hours)
    - Summary: Practicing the "career conversation" via AI Supervisor Role-Play.
    - Assesses: ELO 3.4.2
- Session 2: IDP Final Clinic & "Lightning Briefs" (GOV, 3.5 hours)
    - Summary: Students provide final feedback and make final edits (not the same people they worked with during the first clinic). Then students prepare and deliver a 4-minute brief on their career story, overall goals, 2 "cool opportunities" discovered, and 1 commitment for the next 90 days (either gallery walk, round-robin, or just in groups). Final IDP submitted.
    - Assesses: ELO 3.2.6, 3.2.7
- Session 3: Capstone Close-Out (GOV, 1.0 hour)
    - Summary: Final synthesis connecting the course curriculum to operational reality.

Attachment 5 – Notional Learning Experiences and Assignments

The below are learning experience and assignments that are under consideration for integration into the course and can be modified in the design phase until an agreement is reached between Contractor and Government.

1. Online Foundational Experiences

Experience Title	Core Activity Description	Aligned Objectives (TLO/ELO)
Activity 0.0: The "Give & Get"	Icebreaker to activate the horizontal Guardian network.	*Administrative / Cohort Building*
Activity 0.1: AI Sandbox	Practice using the Persona-Context-Task-Format prompting model to explain SDA.	ELO 2.4.2
Act. 1.1: Scavenger Hunt	Using real-world websites to visualize orbits, debris, and congestion.	TLO 1.1 TLO 1.2
Act. 1.2: Threat Assessment Quiz	An automated check to ensure they can categorize counterspace threats before the wargame.	ELO 1.4.1 ELO 1.4.2
Act. 1.3: Viasat Case Study (or Similar Case Study)	A worksheet analyzing a real-world cyberattack to differentiate SDA facts from Intelligence assessment.	ELO 1.5.1, 1.5.2 ELO 1.6.2
Act. 1.4: Mission to Effect	A translation exercise turning technical jargon into clear "warfighter benefits" for joint partners.	ELO 1.7.5 ELO 1.7.6
Act. 2.2: Personal Mission Statement	A reflective writing task connecting their specific job series to a Guardian Value and a USSF Mission.	ELO 2.5.1 ELO 2.5.2
Act. 3.1: The Resource Safari	An interactive "safari" through the DAF/DoW ecosystem (DAU, AU, Digital University, MyVector, etc.).	ELO 3.1.2
Act. 3.1c: AI Discovery Log	Using AI as a strategic research partner to find "hidden" non-traditional training (podcasts, industry certs).	ELO 3.1.3

Act. 3.2: Mentor Outreach	A practical exercise in drafting a professional subject line and email body to a potential mentor.	ELO 3.3.1, 3.3.2

2. Longitudinal "Bridge" Projects
These start online and culminate in person.

Experience Title	The Online Phase	The In-Person Phase	Aligned Objectives (TLO/ELO)
The Simulated Dossier Project	Groups research a space-faring nation's capabilities, goals, and posture using AI synthesis. (“X Threat/Capability exists in Y sector from Z Country)	This Dossier becomes their "playbook" or "stat card" for the one of the tabletop simulations/ wargame.	TLO 1.8
The Innovation Challenge	Groups brainstorm a solution to the "Debris Tracking Challenge" and use an AI Red Team to find flaws.	Groups present their digital prototype and lead a "Failure Analysis" debrief on the AI feedback.	ELO 2.2.4 ELO 2.4.3
The 18-Month IDP	Students draft their full career plan, including 3 SMART goals and a proactive resilience strategy.	Students undergo a Peer Review Clinic and practice advocating for the plan in an AI Role-Play.	TLO 3.2 ELO 3.2.3

3. In-Person High-Fidelity Experiences
These are the immersive events exclusive to the residential week.

Experience Title	Core Activity Description	Aligned Objectives (TLO/ELO)
Ethical Space Dilemma Tabletop	A Socratic discussion of a historical or notional case study, focusing on dissenting expert advice vs. organizational pressure.	TLO 2.3 ELO 2.3.4
The Scaffolding Simulation	A structured, rules-based tabletop game where teams use their Dossiers to make planning-based decisions in a crisis.	TLO 4.1 ELOs 4.1.1 - 4.1.5

The Strategic Engagement	A "Find a Tool / Find a Problem" mission consisting of a Partner Site Visit and a Senior Leader Brief.	ELOs 4.4.1, 4.4.2
The Dynamic Crisis Sim	A high-intensity, narrative-driven crisis with timed "friction injects" requiring rapid adaptation and formal AAR briefs.	TLO 4.2 TLO 4.3
The Advocacy Rehearsal	An individual simulation where students practice their "career conversation" with a skeptical AI military supervisor.	ELO 3.4.2
The Capstone Debrief	The final synthesis where the class connects the "Tool" from the site visit to the "Problem" from the leader brief.	ELO 4.4.3

Attachment 6 – Part 5352 - Solicitation Provisions and Contract Clauses

DEPARTMENT OF THE AIR FORCE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DAFFARS) PART 5352 Knowledge Center

Revised: June 2024

Subpart 5352.2 — TEXT OF PROVISIONS AND CLAUSES

5352.201-9101 Ombudsman

5352.204-9000 Notification of Government Security Activities

5352.204-9002 Security Incident Reporting and Procedures

5352.209-9000 Organizational Conflict of Interest

5352.209-9001 Potential Organizational Conflict of Interest

5352.217-9000 Long Lead Limitation of Government Liability

5352.242-9001 Common Access Cards (CAC) for Contractor Personnel

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Subpart 5352.2 — TEXT OF PROVISIONS AND CLAUSES

5352.201-9101 Ombudsman

As prescribed in 5301.9103 Solicitation Provision and Contract Clause, insert the following clause: OMBUDSMAN (JUL 2023)

(a) An ombudsman has been appointed to hear and facilitate the resolution of concerns from offerors, potential offerors, and others for this acquisition. When requested, the ombudsman will maintain strict confidentiality as to the source of the concern. The existence of the ombudsman does not affect the authority of the program manager, contracting officer, or source selection official. Further, the ombudsman does not participate in the evaluation of proposals, the source selection process, or the adjudication of protests or formal contract disputes. The ombudsman may refer the interested party to another official who can resolve the concern.

(b) Before consulting with an ombudsman, interested parties must first address their concerns, issues, disagreements, and/or recommendations to the contracting officer for resolution. Consulting an ombudsman does not alter or postpone the timelines for any other processes (e.g., agency level bid protests, GAO bid protests, requests for debriefings, employee-employer actions, contests of OMB Circular A-76 competition performance decisions).

(c) If resolution cannot be made by the contracting officer, the interested party may contact the ombudsman, [Insert names, addresses, telephone numbers, facsimile numbers, and e-mail

addresses of Center/MAJCOM/FLDCOM/DRU/DAFRCO ombudsman/ombudsmen]. Concerns, issues, disagreements, and recommendations that cannot be resolved at the Center/MAJCOM/FLDCOM/DRU ombudsman level, may be brought by the interested party for further consideration to the Department of the Air Force ombudsman, Associate Deputy Assistant Secretary (ADAS) (Contracting), SAF/AQC, 1060 Air Force Pentagon, Washington DC 20330-1060, phone number (571) 256-2395, facsimile number (571) 256-2431.

(d) The ombudsman has no authority to render a decision that binds the agency. (e) Do not contact the ombudsman to request copies of the solicitation, verify offer due date, or clarify technical requirements. Such inquiries shall be directed to the contracting officer.

(End of clause)

5352.209-9000 Organizational Conflict of Interest

As prescribed in DAFFARS 5309.507-2(a), insert the following clause, substantially as written, in Section I:

ORGANIZATIONAL CONFLICT OF INTEREST (JUL 2023) (a) The following restrictions and definitions apply to prevent conflicting roles which may bias the Contractor's judgment or objectivity, or to preclude the Contractor from obtaining an unfair competitive advantage in concurrent or future acquisitions.

(1) Descriptions or definitions:

- "Contractor" means the business entity receiving the award of this contract, its parents, affiliates, divisions and subsidiaries. "Development" means all efforts towards solution of broadly-defined problems. This may encompass research, evaluating technical feasibility, proof of design and test, or engineering of programs not yet approved for acquisition or operation.

- "Proprietary Information" means all information designated as proprietary in accordance with law and regulation, and held in confidence or disclosed under restriction to prevent uncontrolled distribution. Examples include limited or restricted data, trade secrets, sensitive financial information, and computer software; and may appear in cost and pricing data or involve classified information.

- "System" means the system that is the subject of this contract.

- "System Life" means all phases of the system's development, production, or support.

- "Systems Engineering" means preparing specifications, identifying and resolving interface problems, developing test requirements, evaluating test data, and supervising design.

- "Technical Direction" means developing work statements, determining parameters, directing other Contractors' operations, or resolving technical controversies.

(2) Restrictions: The Contractor shall perform systems engineering and/or technical direction, but will not have overall contractual responsibility for the system's development, integration, assembly and checkout, or production. The parties recognize that the Contractor shall occupy a highly influential and responsible position in determining the system's basic concepts and supervising their execution by other Contractors. The Contractor's judgment and recommendations must be objective, impartial, and independent. To avoid the prospect of the Contractor's judgment or recommendations being influenced by its own products or capabilities, it is agreed that the Contractor is precluded for the life of the system from award of a DoD contract to supply the system or any of its major components, and from acting as a subcontractor or consultant to a DoD supplier for the system or any of its major components.

(End of clause)

ALTERNATE I (JUL 2023). As prescribed in DAFFARS 5309.507-2(a)(2), either substitute paragraph (a)(2) of the basic clause with one or both of the following paragraphs, or use one or both in addition to the basic paragraph (a)(2). Use these paragraphs substantially as written.

(a)(2)(i) The Contractor shall prepare and submit complete specifications for non-developmental items to be used in a competitive acquisition. The Contractor shall not furnish these items to the DoD, either as a prime or subcontractor, for the duration of the initial production contract plus (insert a specific period of time or an expiration date).

(a)(2)(ii) The Contractor shall either prepare or assist in preparing a work statement for use in competitively acquiring the (identify the system or services), or provide material leading directly, predictably, and without delay to such a work statement. The Contractor may not supply (identify the services, the system, or the major components of the system) for a period (state the duration of the constraint, however, the duration of the initial production contract shall be the minimum), as either the prime or subcontractor unless it becomes the sole source, has participated in the design or development work, or more than one Contractor has participated in preparing the work statement.

ALTERNATE II (JUL 2023).

As prescribed in DAFFARS 5309.507-2(a)(3), either substitute paragraph (a)(2) of the basic clause with the following paragraph, or add the following in addition to the basic restriction. Renumber the paragraphs as needed if more than one restriction applies. Use this paragraph, substantially as written.

(a)(2) The Contractor shall participate in the technical evaluation of other Contractors' proposals or products. To ensure objectivity, the Contractor is precluded from award of any supply or service contract or subcontract for the system or its major components. This restriction shall be effective for (insert a definite period of time). This does not apply to other technical evaluations concerning the system.

ALTERNATE III (JUL 2023).

As prescribed in DAFFARS 5309.507-2(a)(4), add the following paragraph (b) to the basic clause substantially as written:

(b) The Contractor may gain access to proprietary information of other companies during contract performance. The Contractor agrees to enter into company-to-company agreements to: (1) protect another company's information from unauthorized use or disclosure for as long as it is considered proprietary by the other company; and, (2) to refrain from using the information for any purpose other than that for which it was furnished. For information purposes, the Contractor shall furnish copies of these agreements to the contracting officer. These agreements are not intended to protect information which is available to the Government or to the Contractor from other sources and furnished voluntarily without restriction.

ALTERNATE IV (JUL 2023).

As prescribed in DAFFARS 5309.507-2(a)(5), add the following paragraph (b) to the basic clause. If Alternate III is also used, renumber this to paragraph (c).

(b) The Contractor agrees to accept and to complete all issued task orders, and not to contract with Government prime Contractors or first-tier subcontractors in such a way as to create an organizational conflict of interest.

ALTERNATE V (JUL 2023). As prescribed in DAFFARS 5309.507-2(a)(6), add the following paragraph (b) to the basic clause substantially as written. If more than one Alternate is used, renumber this paragraph accordingly.

(b) The Contractor agrees to accept and to complete issued delivery orders, provided that no new organizational conflicts of interest are created by the acceptance of that order. The contracting officer shall identify the organizational conflict of interest in each order. The Contractor shall not contract with Government prime Contractors or first-tier subcontractors in such a way as to create an organizational conflict of interest.

ALTERNATE VI (JUL 2023). As prescribed in DAFFARS 5309.507-2(a)(7), add the following paragraph (b) to the basic clause substantially as written. If either Alternate III or IV or both are used, renumber this paragraph accordingly.

(b) The above restrictions shall be included in all subcontracts, teaming arrangements, and other agreements calling for performance of work which is subject to the organizational conflict of interest restrictions identified in this clause, unless excused in writing by the contracting officer.

5352.209-9001 Potential Organizational Conflict of Interest

As prescribed in DAFFARS 5309.507-2(b), insert the following provision, substantially as written in Section L:

POTENTIAL ORGANIZATIONAL CONFLICT OF INTEREST (JUL 2023)

(a) There is potential organizational conflict of interest (see FAR Subpart 9.5, Organizational and Consultant Conflicts of Interest) due to (state the nature of the proposed conflict). Accordingly:

(1) Restrictions are needed to ensure that (state the nature of the proposed restraint and the applicable time period).

(2) As a part of the proposal, the offeror shall provide the contracting officer with complete information of previous or ongoing work that is in any way associated with the contemplated acquisition.

(b) If award is made to the offeror, the resulting contract may include an organizational conflict of interest limitation applicable to subsequent Government work, at either a prime contract level, at any subcontract tier, or both. During evaluation of proposals, the Government may, after discussions with the offeror and consideration of ways to avoid the conflict of interest, insert a special provision in the resulting contract which shall disqualify the offeror from further consideration for award of future contracts.

(c) The organizational conflict of interest clause included in this solicitation may be modified or deleted during negotiations.

(End of provision)

ALTERNATE I (JUL 2023).

At the discretion of the contracting officer, substitute the following paragraph (b) for paragraphs (b) and (c) in the basic provision:

(b) The organizational conflict of interest clause in this solicitation may not be modified or deleted.

5352.242-9000 Contractor Access to Department of the Air Force Installations

As prescribed in DAFFARS 5342.490-1, insert a clause substantially the same as the following clause in solicitations and contracts:

CONTRACTOR ACCESS TO THE DEPARTMENT OF THE AIR FORCE INSTALLATIONS (JUN 2024)

(a) The contractor shall obtain base identification and vehicle passes, if required, for all contractor personnel who make frequent visits to or perform work on the Department of the Air Force installation(s) cited in the contract. Contractor personnel are required to wear or prominently display installation identification badges or contractor-furnished, contractor identification badges while visiting or performing work on the installation.

(b) The contractor shall submit a written request on company letterhead to the contracting officer listing the following: contract number, location of work site, start and stop dates, and names of employees and subcontractor employees needing access to the base. The letter will also specify

the individual(s) authorized to sign for a request for base identification credentials or vehicle passes. The contracting officer will endorse the request and forward it to the issuing base pass and registration office or Security Forces for processing. When reporting to the registration office, the authorized contractor individual(s) should provide a valid driver's license, current vehicle registration, valid vehicle insurance certificate, and [*insert any additional requirements to comply with local security procedures*] to obtain a vehicle pass.

(c) During performance of the contract, the contractor shall be responsible for obtaining required identification for newly assigned personnel and for prompt return of credentials and vehicle passes for any employee who no longer requires access to the work site.

(d) When work under this contract requires unescorted entry to controlled or restricted areas, the contractor shall comply with *[insert any additional requirements to comply with AFI 31-101 , Integrated Defense, and DODMAN5200.02_AFMAN 16-1405 , Air Force Personnel Security Program]* citing the appropriate paragraphs as applicable.

(e) Upon completion or termination of the contract or expiration of the identification passes, the prime contractor shall ensure that all base identification passes issued to employees and subcontractor employees are returned to the issuing office.

(f) The contractor shall provide an after-hours contact number or after-hours email in the Emergency Mass Notification System (EMNS) for each of their personnel, whose normal place of duty is on a DoD installation or within a DoD facility. The contractor shall comply with any additional requirements in DAFMAN 10-206 for emergency operational reporting. Foreign Nationals may participate and may remove themselves from the Emergency Mass Notification System at any time. To update information, personnel can access the globe icon on their system desktop screens and choose the "Access Self-Service" option.

(g) Failure to comply with these requirements may result in withholding of final payment.

(End of clause)

Attachment 7 – CMMC

(HAF) OSD Memo - CMMC Implementati

OFFICE OF THE SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing the Cybersecurity Maturity Model Certification (CMMC) Program: Guidance for Determining Appropriate CMMC Compliance Assessment Levels and Process for Waiving CMMC Assessment Requirements

The defense industrial base (DIB) is the target of recurrent and progressively sophisticated cyber attacks targeting Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) processed in, stored on, or transmitted over nonfederal unclassified information systems. These attacks threaten Department of Defense (DoD or Department) mission execution, reduce warfighting capabilities, weaken American technological superiority, and exfiltrate intellectual property and national security information. The Department is undertaking multiple efforts to reduce the risk of cyber attacks to DIB businesses.

Defense contractors and subcontractors are required to safeguard unclassified nonpublic information by applying specified network security requirements, as defined in DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, which includes identified CUI and FCI that resides in or transits contractor unclassified information systems. Title 32 of the Code of Federal Regulations (CFR) § 2002 describes requirements for adequate safeguarding that, in the context of Defense contracts, are implemented through Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. This clause applies to contracts that require the processing, storing, or transmitting of CUI on contractor-owned information systems.

To enhance the security of DoD information and reduce the risk of cyber attacks to DIB businesses, the Department established the Cybersecurity Maturity Model Certification (CMMC) Program. The final CMMC Program rule was published to the *Federal Register* on October 15, 2024 and is codified in Title 32 CFR Part 170. The CMMC Program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding CUI or FCI. The CMMC Program will implement pre-award assessments of contractor compliance with the appropriate information safeguarding requirements. Title 32 CFR § 170 defines applicability of CMMC requirements and Title 48 CFR DFARS provisions and clauses will implement those requirements.

Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, Program Managers and requiring activities shall include the need for CMMC assessments in procurement request and requirement documents in accordance with phase-in timelines described in Title 32 CFR § 170.3. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance to apply when determining the appropriate CMMC assessment level to include in each DoD solicitation and contract. Service and Component Acquisition Executives are authorized to waive inclusion of CMMC assessment requirements in DoD solicitations. Waivers are discussed in Attachment 2.

At the conclusion of the phase-in period, Program Managers and requiring activities will designate a CMMC level for each contract, as appropriate, according to attributes of the information that will be processed, stored, or transmitted on covered contractor information systems, as described in Attachment 1. Service and Component Acquisition Executives may, after following approved procedures, waive CMMC assessment requirements, as described in Attachment 2. A waiver of CMMC assessment requirements does not affect the underlying security requirements, or current policy, that may apply (including, but not limited to, Federal Acquisition Regulation (FAR) clause 52.204-21 and DFARS clause 252.204-7012), which will remain in effect.

Finally, when a requirement is expected to result in award of a non-FAR based grant or other legal agreement, Program Managers and requiring activities are still expected to follow the CMMC Level Determination Guide (Attachment 1) to select an appropriate CMMC level requirement.

The Office of the DoD Chief Information Officer intends to incorporate the attached policies into one or more DoD Instructions, as appropriate. Additionally, the Department will revise DoD Instruction 8582.01 to provide guidance for applying the enhanced protections provided by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, which are carried forward in CMMC Level 3. The CMMC Program Management Office is the point of contact for this effort: osd.pentagon.dod-cio.list.cmmc-mbx@mail.mil. The Office of the Under Secretary of Defense for Research and Engineering will publish and maintain a guidebook with additional details for the application of NIST SP 800-172 at https://aaf.dau.edu/guidebook.

Heidi Shyu
Under Secretary of Defense
for Research and Engineering

JAN 15 2025

Leslie A. Beavers
Acting Chief Information Officer
of the Department of Defense

JAN 13 2025

Dr William LaPlante
Under Secretary of Defense
for Acquisition and Sustainment

Attachments:
As stated

Attachment 1
Cybersecurity Maturity Model Certification Level Determination

Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012 and Federal Acquisition Regulation (FAR) clause 52.204-21 establish the cybersecurity requirements for FAR-based contracts. Title 32 of the Code of Federal Regulations (CFR) § 170.3 (e) describes a phased implementation plan for assessment of compliance with these requirements under the CMMC Program.

Program Managers and requiring activities shall follow the CMMC Program implementation phases defined in Title 32 CFR § 170.3(e). Upon publication of the final Title 48 CFR DFARS rule, 2019-D041, all procurement requests that may result in a contract where the contractor or a subcontractor, at any tier, may have **Federal Contract Information** (FCI), as defined in FAR clause 52.204-7021, residing in or transiting through its information system shall include CMMC Level 1.

One year after publication of the DFARS rule, Program Managers and requiring activities shall also begin to require CMMC Level 2 certification assessments, when appropriate. In two years, Program Managers and requiring activities shall begin to implement CMMC Level 3 certification assessment requirements, when appropriate.

In accordance with DFARS Procedures, Guidance, and Information 204.7303-1(b)(1), the requiring activity must notify the contracting officer when an effort is expected to result in a contract, task order, or delivery order that will involve **covered defense information** (including Controlled Unclassified Information (CUI)) or operationally critical support. Covered defense information is defined in DFARS clause 252.204-7012. In order to appropriately apply information safeguarding requirements, when the effort will involve CUI, the requiring activity must also identify whether CMMC Level 2 self-assessment of certification assessment is the minimum requirement. Contacting Officers will rely on information provided by the requiring activity to communicate the applicable CMMC level requirements to offerors and contractors.

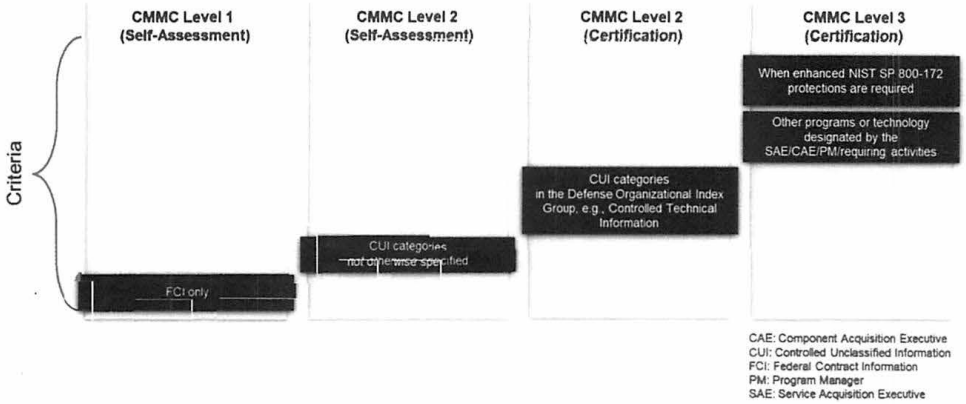
CMMC Level 3 assessments shall be required when DoD policy requires the application of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172. The enhanced protections of NIST SP 800-172 must be applied to safeguard CUI associated with mission critical or unique technologies and programs. Program Managers and requiring activities must also carefully consider the risks associated with the security of the subcontractors' nonfederal information systems in the multi-tier supply chain and provide additional solicitation guidance regarding the extent to which CMMC Level 3 requirements must be flowed down.

The Department is updating DoDI 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, and is developing a Defense Acquisition University guidebook, to include guidance for applying NIST SP 800-172.

DoD Program Managers and requiring activities will use the following CMMC Level Determination Guide to identify the appropriate CMMC level for a given contract. When a contract effort will result in CUI being processed, stored, or transmitted on a contractor information system that meets multiple CMMC level determination criteria, Program Managers and requiring activities shall select the highest applicable CMMC level. The guidance contained herein addresses the minimum required assessment levels and does not preclude selection of a higher CMMC level requirement when security needs dictate.

Until supplanted by a DoD Instruction, this CMMC Level Determination Guide defines the minimum CMMC level requirement. Other DoD policies, regulations, or security concerns may necessitate selection of a higher CMMC level requirement. Service and Component Acquisition Executives may issue supplementary guidance to ensure CMMC requirements are consistently applied, in particular for CMMC Level 3 Certification assessments. Flow-down requirements for all other CMMC assessment requirements are defined in Title 32 CFR § 170.23.

CMMC Level Determination Guide



CMMC Level 1 (Self-Assessment) – Assessed against the FAR clause 52.204-21:

- FAR clause 52.204-21 applies to FCI. This clause does not apply to information provided by the Government to the public, such as on public websites, or simple transactional information, such as is necessary to process payments.

- If the planned contract, task order, or delivery order may require the contractor (or subcontractors at any tier) to process, store, or transmit only FCI in its information system, the appropriate assessment requirement is CMMC Level 1 Self-Assessment.

CMMC Level 2 – Assessed against the NIST SP 800–171:

- DFARS clause 252.204-7012 applies when CUI will be processed, stored, or transmitted on contractor-owned information systems in the performance of a DoD contract and flows down to subcontracts, or similar contractual instruments, as described in DFARS clause 252.204-7012.

- If the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI on a contractor-owned information system, compliance must be assessed against NIST SP 800-171 requirements.

    - **CMMC Level 2 (Self-Assessment)** is the minimum assessment requirement for CUI. It is sufficient only for CUI outside of the National Archive's CUI Registry Defense Organizational Index Grouping. Category markings and definitions may be found on

the CUI Registry at https://www.archives.gov/cui. The Program Manager may elevate the CMMC level if there is high risk to the confidentiality, integrity, or availability of the CUI.

- **CMMC Level 2 (Certification)** is the minimum assessment requirement when the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI categorized under the National Archive's CUI Registry Defense Organizational Index Grouping. Category markings and definitions may be found on the CUI Registry at https://www.archives.gov/cui. CMMC Level 2 certification assessment is performed by third-party assessors employing the methods described in NIST SP 800-171A.

CMMC Level 3 (Certification) – Assessed by DoD officials against select controls in NIST SP 800–172:

- The enhanced protections of NIST SP 800-172 must be applied to safeguard mission critical or unique technologies and programs associated with the following factors/scenarios. Compliance with NIST SP 800-172 is a significant effort. Program Managers and requiring activities must carefully consider the need for safeguarding of the particular CUI to be shared and avoid overuse of the CMMC Level 3 requirement.
  - CUI associated with a breakthrough, unique, and/or advanced technology;
  - Significant aggregation or compilation of CUI in a single information system or IT environment; and
  - Ubiquity – when an attack on a single information system or IT environment would result in widespread vulnerability across DoD.
- The Office of the Under Secretary of Defense for Research and Engineering will publish and maintain a guidebook with additional details for the application of NIST SP 800-172 at https://aaf.dau.edu/guidebook.
- If the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI that requires enhanced protections provided by NIST SP 800-172, then the minimum assessment requirement is CMMC Level 3 (Certification).
  - DoD Program Managers and requiring activities will determine if a contract effort requires the contractor (or subcontractors) to process, store, or transmit CUI within nonfederal unclassified information systems pertaining to the essential technology elements identified for prioritized protection through application of the NIST SP 800-172 requirements described in DoD Instruction 8582.01.
  - When CMMC Level 3 is warranted, a Security Classification Guide must be provided to communicate any CUI distribution limitations or instructions and allow for the segregation of information such that information that need not be covered by CMMC Level 3 can be handled appropriately at levels below CMMC level 3 throughout the supply chain. Failure to do so may result in the CMMC Level 3 requirements being unnecessarily flowed down to all sub-tiers at significant cost to the program.

ATTACHMENT 2
CYBERSECURITY MATURITY MODEL CERTIFICATION WAIVER APPLICABILITY AND REPORTING REQUIREMENTS

Program Managers or requiring activities may request Service Acquisition Executive (SAE) or Component Acquisition Executive (CAE) approval to waive CMMC assessment requirements that would otherwise apply (including invoking lesser CMMC assessment levels), within the parameters below, or as supplemented by policies that SAEs or CAEs may issue. All CMMC waiver requests must be coordinated through the component Chief Information Officer (CIO) prior to SAE or CAE approval. For programs under Defense Acquisition Executive (DAE) oversight, Program Managers shall coordinate waiver requests through the component CIO, Program Executive Officer, CAE or SAE, and the Office of the DoD CIO at osd.pentagon.dod-cio.list.cmmc-mbx@mail.mil prior to DAE approval.

CMMC waivers may be requested and approved for an individual procurement or a class of procurements, and waivers will impact only whether CMMC assessments must be included in solicitation documents and resultant contracts. CMMC assessment waivers do not affect the underlying security requirements of Federal Acquisition Regulation (FAR) clause 52.204-21, Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, or National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, when applicable pursuant to DoD policy. All agencies are required by Title 32 of the Code of Federal Regulations (CFR) § 2002 to use NIST SP 800-171 when establishing requirements to protect Controlled Unclassified Information (CUI) on nonfederal information systems. Refer to DoD Instruction 8582.01, *Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information*, for additional guidance on security of non-DoD information systems processing unclassified DoD information.

Waiver Reporting Requirements:

SAEs and CAEs will report CMMC waiver data quarterly to the Under Secretary of Defense (USD) for Acquisition and Sustainment, the USD for Intelligence and Security, the USD for Research and Development, and the Office of the DoD CIO. Reports can me made via postings to osd.pentagon.dod-cio.list.cmmc-mbx@mail.mil. The report will enumerate all contracts awarded with CMMC assessment requirements waived, by the certification level that would otherwise have applied, and will identify common Product Service Codes or other relevant information that may explain market circumstances necessitating such assessment waivers.

Phase-In of CMMC Assessment Requirements, Including Waiver Process:

Program Managers and requiring activities should identify information security requirements for the types of information most likely to be associated with the planned contract effort. When market research indicates that including a CMMC assessment requirement may impede ability to generate robust competition or delay delivery of mission critical capabilities, the SAE, CAE, or DAE may approve requests to waive inclusion of CMMC assessment requirements. SAEs and CAEs must carefully weigh the risk of potential loss of CUI associated with mission critical capabilities before granting a waiver. SAEs and CAEs must recognize the following waiver limitations and may supplement this guidance with specific information, formatting, and coordination requirements.

1. CMMC Level 1 requirements: CMMC Level 1 is a self-assessment requirement designed to provide added insight into or assurance of the offeror's compliance with requirements defined in FAR clause 52.204-21 for the safeguarding of Federal Contract Information (FCI). This is the most basic level of cybersecurity posture. There are no circumstances likely to warrant approval of requests to waive CMMC Level 1 requirements.

2. CMMC Level 2 requirements: CMMC Level 2 can be a self-assessment requirement or an independent third-party assessment.

    a. Effective September 29, 2020, DFARS Subpart 204.73, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, was amended to require the inclusion of DFARS clause 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*, in all solicitations, except those solely for the acquisition of commercial off-the-shelf items. This provision requires offerors to provide a current NIST SP 800–171 DoD Assessment on record, prior to contract award, whenever the offeror is required to implement NIST SP 800–171, pursuant to DFARS clause 252.204–7012. Due to this pre-existing minimum requirement for a Basic self-assessment under DFARS 252.204-7019 and the ability to establish corrective Plans of Action and Milestones, there are no circumstances likely to warrant approval of requests to waive CMMC Level 2 self-assessment requirements.

    b. In rare circumstances, such as when seeking competition from non-traditional DoD sources, waivers may be warranted for CMMC Level 2 third-party assessment requirements. Such waivers are not appropriate for contracts requiring performance by a cleared defense contractor. Approved waivers on a class basis must include a planned expiration date and guidance for requiring CMMC certification in subsequent solicitations. In all such cases, the solicitation must include a requirement to submit alternate protection plans for securing FCI or Controlled Unclassified Information (CUI) data. The alternate protection plans must be evaluated as part of the selection process.

3. CMMC Level 3 requirements: Level 3 requirements are intended to protect CUI associated with the Department's mission critical technologies and programs and result in an assessment performed by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center. In rare circumstances, waivers may be warranted for CMMC Level 3 third-party assessment requirements: such waivers, however, are not appropriate for contracts or work statements requiring access to both unclassified and classified DoD information.