PERFORMANCE WORK STATEMENT (PWS)

FOR

STAR Follow On

Commented [MH1]: Will be updated.

27 August 2025

Delta 11

Template AO: HQ STARCOM/ES

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 Business Operations.

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, Title50,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.

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*
A	dd Apr 24	Final RFP Release.

Commented [MH2]: Will be updated once first draft is complete

Table of Contents

1 Introduction/Background 1
1.1 Mission Overview 1
1.2 Scope 1
2 General Requirements 1
2.1 Non-Personal Services 2
2.2 Contractor Management 2
2.3 Contractor Personnel, Disciplines, and Specialties 3
2.4 Location and Hours of Work 4
2.5 Travel / Temporary Duty (TDY) 5
2.6 Security and Safety 6
2.7 Manpower Reporting 10
2.8 Documentation 10
2.9 Performance Evaluation. 11
2.10 Government Furnished 12
3 Performance Requirements 12
3.1 Space Aggressor EW Support 12
3.2 Space Aggressor OW Support 21
3.3 Space Cyber Range Support 25
3.4 Transition 30
3.5 Associate Contractor Agreements (ACA) 31
3.6 STARCOM Directed Meetings/Events 32
4 Applicable Publications 32
5 Deliverables 34
6 Services Summary 49
Appendix A: Mission System Inventory Descriptions 50
Attachment 1 – Government Furnished Property 56
Attachment 2 – Government Furnished Material 57

Performance Work Statement (PWS)

1 Introduction/Background

This Performance Work Statement (PWS) outlines the requirements for providing comprehensive support to the 527th Space Aggressor Squadron (527 SAS), the 57th Space Aggressor Squadron (57 SAS) and the 33rd Range Squadron (33 RGS) in their respective missions to prepare Joint Forces and Coalition Partners for operations in contested space environments. As key components of the United States Space Force's (USSF) mission qualification and professional adversary force, these units require robust support to effectively execute their missions and enhance their ability of replicating the threat, ultimately ensuring allied victory in the space domain. This PWS defines the specific tasks and deliverables required to enable all three units to achieve these objectives.

1.1 Mission Overview

To prepare Joint Forces and Coalition Partners for operations in contested space environments by providing realistic, relevant, and integrated space threat replication and support to the 527 SAS, 57 SAS and 33 RGS.

1.2 Scope

This contract will provide non-personal services through subject matter experts in the following areas: SATCOM, EA, GPS EA, Offensive Cyber Operations (OCO), intelligence product generation, and OW. This includes support to mission planning, system support, development, testing, maintenance, education, mission qualification, and training of Space Aggressors.

Support includes programs identified as Sensitive Compartmented Information (SCI) and Special Access Required (SAR) administered under the enhanced security guidelines & procedures authorized by Department of Defense DODI 5200.01 (DoD Information Security Program and Protection of Sensitive Compartmented Information) and AFI 16-1404 (Air Force Information Security Program).

Future work options are included to provide flexibility in adapting to evolving mission requirements driven by the anticipated growth of supported units. These options encompass potential future tasks, services, and capabilities that may become necessary to maintain optimal support and performance as the operational environment expands. Exercise of these options will be subject to mutual agreement, incorporating factors such as evolving mission needs, technological advancements, and available resources. This mechanism allows for proactive and agile adaptation of the contract to ensure continued effective support to the growing user base and to seamlessly integrate emerging requirements without the need for extensive renegotiation.

Identify if this requirement includes any Mission Essential Services, submission of ME plan IAW DFARS 252.237-7023

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 **Period of Performance** is as follows:
Base Year: Contract start – 31 Oct 2027
OY1: 01 Nov 2027 – 31 Oct 2028
Optional Extension up to 6 Mos: 1 Nov 2028 – 30 Apr 2029 (only for emergencies)

DRAFT

2.1 Non-Personal Services

The government will not supervise contactor employees or control the specific methods by which the contractor performs the required tasks. The government will not assign tasks to individual contractor employees or prepare their work schedules. However, to ensure clarity, facilitate effective communication, and align efforts with mission objectives, the government may provide amplifying guidance and intent related to specific project, tasks, or sections within the 527 SAS, 57 SAS, and 33rd RGS. This guidance will primarily be directed at contactor management and task leads. However, government personnel may engage directly with contractor employees involved in specific projects to discuss technical matters, clarify requirements, and provide feedback on work in progress. These interactions are intended to enhance understanding and collaboration and should not be construed as direct supervision or task assignment. The contractor remains responsible for managing its employees, assigning tasks, and determining the appropriate methods to achieve the required outcomes.

The contractor shall ensure its employees understand the prohibitions imposed on the government regarding personal services contracts. 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 purpose 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
AA01 – 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.

To enhance performance and support the 527th SAS mission, the contractor may request approval for its employees to attend government sponsored, or government provided training session focused on software, administrative procedures, or other directly relevant areas. The contractor may also request approval for employees to attend third party provided off site seminars and classes that directly contribute to the contractor's ability to fulfill the requirements of this PWS. All requests for training attendance must be submitted to the 527th SAS leadership (or their designee) for review and approval at least 140 business days prior to the scheduled event. Approval will be granted only if the training demonstrably enhances the Contractor's ability to support the 527th SAS mission, is offered at no cost to the government (unless otherwise approved in writing by the Contracting Officer or Contracting Officer Representative), and aligns with the overall training objectives of the 527th SAS. The contractor bears the responsibility for any costs associated with unapproved training.

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
AA02 – 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. The contractor shall provide three task leads to oversee, support, and assisting in EW/OW and Cyber services working as teammates.

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.

DRAFT

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. Additionally, the Government reserves the right to request the removal and replacement of any Contractor personnel whose performance, attendance, or lack of responsiveness demonstrably hinders the 527th SAS mission. This includes, but is not limited to, instances of: (a) documented and repeated unavailability during scheduled work hours; (b) failure to provide timely and accurate information regarding project status or whereabouts upon request; (c) repeated failure to meet agreed-upon deadlines; or (d) any other behavior that negatively impacts the Government's ability to effectively execute its mission. In such cases, the Government will provide written notification to the Contractor, outlining the specific concerns. The Contractor shall provide a replacement within 14 business days of the notification. The Government's decision regarding removal and replacement is final and not subject to protracted legal challenges, provided the removal is based on a good-faith assessment of the Contractor's personnel's impact on mission effectiveness.

2.4 Location and Hours of Work

The primary work location under this PWS is anticipated to be at Bldg. 815 and 24 on Schriever SFB, and at various Contractor and Government facilities. However, the Government reserves the right to designate alternate work locations, including other Government facilities or approved Contractor sites, as necessary to support mission requirements. The Contractor shall comply with all Government directives regarding work location. The Government will provide reasonable notice to the Contractor of any changes to the primary work location, except in cases of urgent operational needs, where shorter notice may be required. The Contractor shall generally support a normal work week of 40 hours per week. Normal workdays are eight (8) hours per day, Monday through Friday, except US Federal Holidays. Mission requirements may be dictated other than Monday through Friday. The units may need to take basing actions, for example the 57 SAS is schedule to work from Kirtland AFB, NM starting in CY27.

2.4.1 Building Access

The Government will provide Contractor personnel unescorted access to Bldg 24 consistent with task requirements. Access to Government facilities, documents and systems will be in accordance with the DD Form 254 and paragraph 2.6.

2.4.2 Morale Events

There may also be occasions when Contractors are invited to participate in morale and recreational activities (e.g., holiday parties, golf outings, sports day and other various social events). Under these circumstances, Contractor employees shall comply with individual company policy in accordance with company compensation system. Because the Government does not have an employer/employee relationship with Contractor employees, it is not authorized to grant administrative leave or expend Government resources to compensate Contractor employees for hours expended on activities not included in the PWS.

2.4.3 Closures

For closures affecting the availability of the Government site (e.g., weather closures, a National Day of Mourning, etc.), the Government will notify the Contractor through normal means such as the Snow Call Line and local news outlets, or via email from the COR or CO. During such closures, Contractor personnel may telework if they have a COR-approved telework request in place and coordinate with the assigned section.

2.4.4 Teleworking

Commented [MH3]: Need to look at this when compared to the old PWS

DRAFT

Telecommuting/telework is defined as authorization for an employee that works at the United States Government (USG) location, to work at an alternate location, i.e., at the employee's home or Contractor location, either routinely or situationally. Contractor-designated location is defined as a contractor-identified place of performance for specific employees, i.e., not at the USG location. There are two types of telecommuting/telework; 1) routine telework in which telework occurs as part of an ongoing, regular schedule within the designated installation operating location area, and 2) situational telework that is approved on a case-by-case basis, where the hours worked were not part of a previously approved, ongoing and regular telework schedule, to include pandemic situations and remote telework (teleworking outside the operating location area), and other non-routine telework situations.

Either telework option will be concurred by Government requirements owners and submitted to the COR. Routine telecommuting/telework will be approved by the COR or the location specific alternate COR. Situational telecommuting/telework requests will be approved by the CO. To obtain approval for teleworking, the Contractor shall submit a teleworking request with appropriate rationale in writing. This request shall include the Contractor's ["lead's", "Project Manager's", "Task Lead's", etc.] approval, as well the primary Government customer's approval, if different than the COR, when the request is submitted to the COR for approval.

Telecommuting/telework is generally customer-specific, and all telework approved equipment must be authorized by the Government for use. Regardless of work location, the Contractor shall maintain availability during core hours via e-mail, Government approved video conferencing, and phone. The Government will not assume operating costs associated with the Contractor using an alternate worksite; all telecommuting/ telework expenses for Internet, telephone connectivity, and other equipment services shall be borne by the Contractor. Any costs related to maintenance required for remote telework Government Furnished Equipment not due to negligence, to include shipping costs (if required), will be paid by the Government. The Contractor shall provide a written request with appropriate rationale for COR or alternate COR approval prior to any telecommuting.

Teleworking is not authorized for classified work. Authorized telework locations do not abrogate the Contractor's requirement for complying with the protection of information IAW DoD, USAF, and USSF regulations, Security and Protection of Information sections of this PWS, contract clauses or the DD Form 254.

2.5 Travel / Temporary Duty (TDY)

Commented [MH4]: This needs to be compared to the old PWS

Travel may be required inside the Continental United States (CONUS) and Outside the Continental United States (OCONUS) on a temporary basis to accomplish the mission. All travel will be at the direction of the Government and reimbursed/accounted for as part of the FFP NTE travel Contract Line-Item Number (CLIN). Approximately 100 days of travel is required per year.

Any travel required to fulfill the tasks within this PWS shall be performed IAW the Joint Travel Regulation (JTR) is not subject to profit and must be initially coordinated with the COR prior to approval. The Contractor shall submit requests and obtain Government approvals for all travel prior to purchasing refundable tickets. Travel will be for purposes such as exercise and mission support and indicated in paragraph 3 of the PWS. The Contractor shall include estimates for all allowed travel costs. If some authorized costs are not included in the request, the Contractor shall state the reasons why the costs are not included in the estimate and invoice. The Contractor shall provide receipts for all expenses incurred and shall follow the JTR. Local area travel is not reimbursable. Local area is a 150-mile radius of Schriever AFB. Any remaining funds will be de-obligated to the buying activity.

Deliverable:
AA03 Travel Report
For all trips, the Contractor shall provide a trip report within ten (10) business days of the return date from travel. Extensions may be granted by the COR on a case-by-case basis. As a minimum, trip reports will include the objectives and outcomes of the trip. Trip reports do not have a specific format and may range from an email to a formal presentation depending on the type of trip.

Commented [MH5]: Keep, but clean up

2.6 Security and Safety

Commented [MH6]: This section needs to be checked with the old PWS

2.6.1 Facility Clearance

The contractor shall possess or obtain a facility clearance at the classification levels specified in the workload data.

The contractor shall apply for personnel security clearances within five days after receipt of the facility clearance or within 30 days after award of the contract if the contractor possesses a facility clearance.

The contractor shall comply with all Schriever Space Force Base (SSFB) and USSF security requirements. SSFB contains a restricted area and Bldg. 24 is a controlled area. In both areas special security procedures are used to deter espionage, sabotage, and theft of USAF/USSF resources. The contractor shall be responsible for security of their work areas in cooperation with applicable base agencies.

The contractor shall be advised that vehicles entering or leaving SSFB are subject to search by the 50th Security Forces Squadron (50 SFS) at their discretion. Drugs, firearms, or other weapons are strictly prohibited and not allowed on SSFB. If found, the individual may be barred from future entry, impacting the contractor ability to meet requirements.

The contractor shall be responsible for all costs incurred by the contractor associated with security requirements including submission of necessary security investigation paperwork, routine entry/exit delays, and operational delays due to contingencies or exercises, are to be anticipated by the contractor.

The contractor shall initiate unescorted entry authorization requests no later than 7 calendar days after their start date, if access to restricted/controlled areas is required IOT perform the tasks described in this PWS,

The contractor shall, always, display restricted/controlled area badges on their outer garments above the waist when inside the restricted/controlled area, Contractor personnel shall remove and secure the restricted/controlled area badge immediately upon departure from the restricted/controlled area to prevent loss. Incidents of a person not properly displaying badges or violating escort procedures (e.g., working out of view of escort) shall be treated as a breach of security and that person shall be susceptible to apprehension, search and detainment. Any person inside a restricted/controlled area without a restricted/controlled area badge will be detained or apprehended, searched, removed, and turned over to appropriate authorities for disposition.

DRAFT

If the contractor is not issued a Restricted Area Badge (RAB) they shall be issued a visitor badge and will be under direct surveillance, at all times, of a USG/Contractor employee possessing a restricted/controlled area badge with escort authority if the contractors require escorted entry.

The contractor shall comply with all applicable security regulations including the restricted/controlled area badge which shall only be valid for the contractor's term of employment or for the duration of the contract, whichever is shorter. Upon contractor termination, the contractor shall surrender the CAC and restricted/controlled area badge to 527 SAS Security Manager within one business day. The contractor shall immediately report the occurrence of any lost badge to the 527 SAS Security Manager and COR within one workday of loss. If 527 SAS Security personnel are not available, the contractor shall report the loss directly to 50 SFS within one workday of loss. The contractor shall not be issued a replacement badge until reporting procedures are satisfactorily completed.

The contractor shall be advised that delays can be anticipated at the entry control point each time an individual enters the restricted/controlled area. These delays are a routine matter when the 50 SFS and/or USAF/USSF search vehicles, hand carried items, check badges, and credentials.

The contractor shall be responsible for protection of USG information, property, equipment and resources that are generated, issued, or supplied under the terms of this contract IAW DoDM 5220.32V2 _AFMAN16-1406V2, *National Industrial Security Program: Industrial Security Procedures for Government Activities,* and AFMAN 16-1404 V1-3, *Air Force Information Security Program*.

The contractor shall enter into a security agreement with the SAFB installation commander. This agreement shall be directive on the contractor. The contractor shall coordinate security matters with the 527 SAS Security Manager and P-S GAR/IP (Schriever). Each eligible contractor employee shall personally report to the 527 SAS Security Manager for completion of the AF Form 2586, Unescorted Entry Authorization Certificate. Contractor employees shall not be allowed unescorted entry to SSFB secured area/buildings until these procedures have been completed. Site activities shall operate with notification of WG/IP and adherence to all guidance

2.6.1 DD Form 254

The contractor shall be provided access to applicable USG facilities. The contractor will be allowed non-escorted access to Government buildings on Schriever SFB, and other sites consistent with task requirements. Access to Government facilities, documents, and systems shall be in accordance with (IAW) the approved Department of Defense (DD) Form 254 – Contract Security Classification Specification, Department of Defense. Employees are subject to all regulations and directives governing the activities of personnel on Government installations, as well as all health and safety directives imposed.

The contractor security manager shall coordinate with the 527 SAS security manager to obtain access and badge information.

The contractor shall coordinate with the Contracting Officer's Representative (COR) to ensure there is no interference with current operations during the transition period and until facility access is granted.

The contractor shall fully participate in all PS-G or Higher Head Quarters (HHQ) directed exercises/inspections to the level dictated by the scenarios in progress. The contractor shall fully participate in all host base exercises and inspections, except as determined by the PS-G commander. This support will be required on a non-mission interference basis during normal contractor duty hours.

The contractor shall not increase manpower or man-hours during exercise participation unless specifically stated in this PWS or authorized by the CO.

2.6.2 Security and Training

The contractor shall identify an individual to perform the duties of Security Manager who shall obtain appropriate personnel security clearances for employees. The Security Manager shall coordinate with 527 SAS Security Manager on all security related issues.

The contractor shall possess a facility clearance at the classification level of “TS” IAW the DD254 at the time of contract award.

All contractor personnel shall have all the clearances as required in DD254. Contractor employees whose duties require access to restricted areas or classified information shall possess a minimum of Secret security clearance unless otherwise noted. The maximum-security level is TS/SCI. 527 SAS will provide additional security clearance information as required.

The Contractor shall comply with the DD Form 254 security requirements. See the DD Form 254 for OPSEC, COMSEC and NATO requirements and guidance.

At a minimum, the contractor shall complete the following courses via the MyLearning on-line access, or classroom attendance within 30 days after contract award. The contractor shall also comply with all required 527 SAS security procedures training. Other training may be required at the direction of the COR.

Course	Frequency	Method
a. OSI/Counterintelligence (INTEL) Brief	Annual	Classroom
b. DoD IAA Cyber Awareness Challenge	Annual	MyLearning
c. Restricted Area Escort Training	Annual	CBT
d. Derivative Classification	Annual	CBT
e. Insider Threat Awareness	Annual	CBT
f. Unauthorized Disclosure of Classified Information and CUI	Annual	CBT

Contractor must comply with foreign travel training required by location as stated in the DoD foreign travel guide (https://www.fcg.pentagon.mil/fcg.cfm)

Contractors may request Antiterrorism Level I training from a 50 SW certified Anti- Terrorism Officer (ATO). Should the contractor choose to complete this training, they must make their request to the 527 SAS COR and the 527 SAS COR will coordinate training locations and times with the installation Antiterrorism Program Manager. Regardless of training, contractors will report suspicious activity to Security Forces (567-6464) or the AF Office of Special Investigations (554-2822).

DRAFT

After contract award, if any of the Government-provided mission support systems change, or new systems are added, the Government will provide initial training upon approval of the COR and direction of the CO. The contractor shall attend training as approved by the COR and directed by the CO. After initial training is completed, the contractor shall be responsible for re- training and training new contractor employees.

The contractor shall attend other training for support provided. This other training includes mission support, geographical-specific, security policy, new equipment, etc. Other training includes 527 SAS provided Mission Qualification Training (MQT), Crew Chief Upgrade Training and instructor qualification. This training will start at phase-in and will be completed within 45 days after contract award.

The contractor shall ensure their employees stay current and proficient in their areas of responsibility.

The contractor shall ensure personnel accessing information systems in the performance of this contract have proper and current cybersecurity certifications to perform support functions IAW DoD 8570.01-M, Information Assurance Workforce Improvement Program and AFMAN 17-1303, Cybersecurity Workforce Improvement Program. The contractor shall authorize certification release for all applicable personnel, whenever a certification is issued or renewed, to DoD/DMDC via https://www.dmdc.osd.mil/milconnect.

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 any CUI information, it shall protect and disseminate that information per the controls required by DoDI 5200.48. 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.

Commented [JT7]: 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 (DF ARS) clause 252.204-7012, *Safeguarding Covered Defense Information and C)iber Incident Reporting*. This clause applies to contracts that require the processing, storing, or transmitting of CUI on contractor-owned information systems.

Upon publication of the final Title 48 CFR DFARS rule, 20 I 9-D04 I, Program Managers and requiring activities shall include the need for Cybersecurity Maturity Model Certification assessments in procurement request and requirement documents in accordance with phase-in timelines described in Title 32 CFR § 170.3. (See embedded doc at the end of the template)

2.6.4 Special Access Programs (SAP)

Access to special access programs (SAPs) and Alternative Compensatory Control Measures (ACCMs) is required. The Contractor's assigned personnel shall have been granted a final TOP SECRET security clearance with eligibility for access to Sensitive Compartmented Information (SCI) and have previous experience working Special Access Programs (SAPs). All personnel are required to submit a SAP Pre-Screening Questionnaire (PSQ) in accordance with DoDM 5205.07 V2 to the Government Program Office and follow procedures outlined in DODM 5200.01 Volume 3. Personnel will be required to consent to and successfully complete a Government Counterintelligence Scope Polygraph. Requests for waivers of SAP experience must be submitted in writing; the Contracting Officer will provide a decision on the request within six (6) working days. Government security officers will determine whether prospective personnel meet the personnel security requirements for any task.

Commented [JT8]: Add ref to Department of Defense Manual (DODM) 5200.01 vol 3 in para 4.

2.6.5 Personnel Security Program

The Contractor shall establish and maintain a personnel security program to support the contract. The Contractor's assigned personnel shall establish and maintain eligibility for access to TOP SECRET Sensitive Compartment Information (SCI) and participate in the Government Counterintelligence Scope Polygraph Program. Government security officers will determine whether the Contractor's personnel meet the personnel security requirements for the tasks under this contract; no costs will be reimbursed related to providing personnel who fail to meet the security requirements.

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:
AA04 – Non-Disclosure Agreement

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.

2.6.7 Counterintelligence Cooperation

Attend mandated CI briefs/events.

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

DRAFT

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.

2.9 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 areas, 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.

DRAFT

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, office space, communications capability and information for 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.

2.10.2 Government Furnished Resources.

The Government will furnish up to workspaces in the MSF, Bldg 24, Bldg 815, & Bldg 442 associated desks, chairs, computers connected to internet, use of telephones, copier and fax machines. Any equipment is considered incidental to performance location.

Commented [MH9]: This needs to be updated

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.

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.

Commented [MH10]: We will need to review the verbiage after the initial draft to either avoid A&AS or put that into it's own CLIN for review.

3.1 Space Aggressor EW Support

Commented [MH11]: Created w/AI. Needs thorough review.

3.1.1 Intel

Research and network system subject matter on intelligence community Information Systems (IS), (i.e. Joint Worldwide Intelligence Communications System (JWICS)) to create and present briefings and white papers to Air, Space, and Cyberspace operations professionals.

Create and present weekly classified intelligence briefs focused on space and space control activities conducted by U.S. adversaries over the period of interest. The briefings shall include a technical analysis of the tactics, system, and operator proficiency demonstrated by the adversary during the observed operation. 527 SAS will provide slide format to be utilized for content.

Provide intelligence briefings, instruction, and advisory support to various training for SAS operators and external customers. This shall include specific threat briefings that are tailored to a specific training audience and their system.

DRAFT

Support exercise planning for Master Scenario Event List builds for threats to be injected into training with modeling and simulation. Travel may be required and will be conducted in accordance with PWS para 2.5.

Maintain a database of observed adversary TTPs, and mission systems to support creation and validation of Space Aggressor tactics. SIPR and/or JWICS will be utilized as the repository for this database. These TTPs shall be updated in the Space Aggressor Adversary Threat Replication Guide (ATRG) and space threats brief quarterly.

Support the evaluation of new military systems and commercially available technologies for the potential threat(s) they may present to U.S./Allied forces. Travel may be required and will be conducted in accordance with PWS para 2.5.

Support threat intelligence community conferences, cross-talks, and Weapons School (Delta 1) syllabus reviews.

Develop/recommend implementation plans for applying intelligence information and procedures to SAS projects to support military training and exercises.

Attend conferences for exercise planning as requested by the Government. Examples include: Deconfliction Conferences, Combined Force Space Component Command, J2 (Intelligence) conferences, NRO Threat Conferences, Space Control Working Group, etc.). Notify the Government COR of scheduling conflicts for personnel to support missions/exercises/training as needed.

Performance Standards
a) Standard: The Current Intelligence Briefings shall include a technical analysis of the tactics, system, and operator proficiency demonstrated by the adversary during the observed operation IAW unit requirements and Intel Flight SOI.
b) Standard: Weekly CIB created and presented 90% of the time.
Deliverable
A001: Weekly Classified Intelligence Briefings on Adversary Space Activities
A002: Tailored Threat Assessments for Specific Training Audiences

3.1.2 Mission Planning

Support the planning and scheduling of exercises that contain SATCOM, ASN, Orbital Warfare, and GPS EA. Note this list may not be all inclusive

Coordinate with training audiences identified by the Government to provide support request forms. Process received support request forms and identify 527 SAS support requirements with training audiences (such as via teleconference). Provide Government with exercise details to enable 527 SAS to adjudicate exercise and event support and its extent; provide recommendation on 527 SAS support based upon personnel and equipment availability, prioritization based on higher headquarter guidance, and feasibility.

Schedule and notify 527 SAS members for exercises and events based on their availability and certification

DRAFT

Update Government documents and trackers with information on upcoming exercises and events, both approved and pending; synchronize and inform 527 SAS members with updated information on upcoming exercises and events, both approved and pending.

Create and support the drafting/staffing/tracking of exercise approval packages. Government review and approval is required before submission to external agencies. Note: staffing packages typically require a long lead time to ensure approvals are received prior to mission need date.

Support drafting/staffing/tracking of GPS EA requests. Produce GPS RPM interference contours and GIANT Jammer to Signal ratio (J/S) contour plots. Utilize Government provided hardware/software to complete this task. Upon Government review and approval, submit packages in accordance with CJCSM 3212.03E (*Performing Electronic Attack in the United States and Canada for Tests, Training, and Exercises*).

Support drafting/staffing/tracking Counterspace Activity Approval Packages (CAAPs). Upon Government review and approval, submit in accordance with Office of the Deputy Secretary of Defense Policy 070640-19 (*Testing, Training, and Exercising of Space Control Electronic Warfare*), Chairman of the Joint Chiefs of Staff Instruction 3320.01D (*Joint Electromagnetic Spectrum Operations*), and AFSPCI 10-211 (*Counterspace Activity Approval Package*) Chapter 4.

Support drafting/staffing/tracking Ultra-High Frequency (UHF) SATCOM EA requests, Satellite Access Requests, Deconfliction Support Request (DSR), and other planning products deemed necessary by the Government. Government review and approval is required for release to any external agencies. SATCOM EA requires close coordination with the 25th Space Range Squadron and with other agencies dependent upon the exercise requirements.

Draft and submit Range Request Forms (RRF) and Operations Requests (OR) to 25 SRS or appropriate range organization after Government review and approval.

Review the 25 SRS published Operations Directives (OD) to ensure Space Aggressor exercise requirements are met. Advise SAP and the Aggressor Mission Commander of any discrepancies, errors, and potential conflicts with Aggressor requirements and resources.

Coordinate with Regional SATCOM Support Centers (RSSC), satellite owner/operators, Space Delta 5 (DEL 5) Radio Frequency Deconfliction, Combined Forces Space Component Command (CFSCC), and other external agencies as required to ensure requests are received and processed. Notify the Government of any issues that may impact timeliness or performance.

<u>Performance Standards</u>

a) Standard: The contractor shall ensure that approval packages or operations requests (to include but not limited to CAAP, EA Request, DSR, and Satellite Access Request) are submitted and accepted prior to the deadlines set by the Government to enable mission requirements set by the Government.
b) Standard: The contractor shall inform the Government if any approval packages or operations requests (to include but not limited to CAAP, EA Request, DSR, and Satellite Access Request) are delayed or at risk of being delayed no later than 10 days prior to deadline.

DRAFT

c) Standard: The contractor will provide the Government with GPS RPM interference contours and GIANT Jammer to Signal ratio (J/S) contour plots within 7 days of request.
d) Standard: The contractor shall process request forms and update Government documents and trackers within 5 business days of receipt and will schedule and attend a meeting with training audiences within 15 business days of receipt, pending training audience availability.
e) Standard: The contractor shall schedule and notify 527 SAS members for exercises and events based on their availability and certification within 10 business days of exercise or event approval by the Government.
f) Standard: The contractor shall update Government documents and trackers with information on upcoming exercises and events, both approved and pending, with updates within 5 business days of receipt of changes.
Deliverable
A003: Exercise Approval Packages (CAAPs, EA Requests, etc.)
A004: Operations Requests (ORs)
A005: Operations Directives (ODs) Review Reports

3.1.3 Adversary Replication

Perform analyses of adversary capabilities and limitations IOT assess effectiveness against U.S. military systems. Such analyses will be used to develop Aggressor CONOPS and TTPs for their replication of these threats against space systems. These analyses will involve technical and engineering assessments of: (1) U.S. and foreign space systems, (2) communications requirements to effect connectivity between elements of space systems, (3) hardware and software for signal generation, verification and electronic support, (4) proof-of- concept tests or demonstrations, and (5) integration of SATCOM and information technology (IT) systems for network development and exercise employment.

Identify and recommend solutions to 527 SAS operational capability shortfalls while minimizing schedule, cost, and technical risks.

Develop and recommend implementation plans for applying intelligence information and procedures to 527 SAS projects ISO military training and exercises.

Research the availability, cost, and procurement of commercial off the shelf components to create systems needed by the 527 SAS. The contractor shall assist in the assembly, test and checkout of these procurements and integrating them into other 527 SAS systems.

Draft appropriate training, job aids, checklists, and operating manuals for new systems to 527 SAS for Government review and approval. The contractor shall also provide training and operations oversight during the initial fielding of these new systems.

Performance Standards
a) Standard: The contractor shall identify and recommend solutions to 527 SAS operational capability shortfalls while minimizing schedule, cost, and technical risks.

b) Standard: The contractor shall assist in the assembly, test and checkout of these procurements and integrating them into other 527 SAS systems IOT meet operational requirements and tempo.
Deliverable
A006: Aggressor CONOPS Documents
A007: Adversary TTPs Database Updates
A008: Implementation Plans for Applying Intelligence
A009: Commercial Off-the-Shelf Component Procurement Reports

3.1.4 Periodic Maintenance Inspections (PMI) and Post Deployment Inspections (PDI)

Perform PMIs and PDIs that include recommendations for ordering replacement parts and installing replacement parts (such as waveguides, transit cases, signal generation electronics, portable electrical generators, travelling wave tube amplifiers, various antennas, etc.), creating and maintaining a periodic maintenance schedule (such as calibrations, etc.), and troubleshooting in the event of a system failure or fault.

Support packing such electronics & equipment as listed in APPENDIX A for air freight and ground-based shipment, and supporting forces deployed with reach-back technical support.
Maintain the equipment listed in APPENDIX A as well as new equipment that may be purchased by the 527th SAS. For any new equipment not listed in APPENDIX A, the appropriate technical orders and maintenance documentation will be provided to the contractor. In the event new equipment is procured by the USG, the USG employees along with the contractor shall be provided training.

Provide initial assessment of equipment mission capability (MISCAP) no later than five (5) business days upon return from exercise support and, if necessary, troubleshoot the cause of a system fault/failure. The contractor shall identify whether the system can be restored to mission capability with organic squadron maintenance capabilities. When repairable, the contractor will repair equipment once parts are available, and installations of parts have been appropriately scheduled.

Performance Standards
a) Standard: Provide an initial assessment of equipment mission capability within 5 business days from return from exercise support. If necessary, troubleshoot cause of system fault/failure and identify if the system can be restored to mission capability with organic squadron maintenance capabilities.
b) Standard: All mission systems are available for exercise support or deployment when parts are available, and installations of parts have been appropriately scheduled
c) Standard: Mission Capability data provided to 527 SAS leadership at weekly DO synch and/or Staff Meeting.
Deliverable
A010: PMI/PDI Reports
A011: Equipment Packing and Shipping Documentation
A012: Reach-back Technical Support Incident Logs

3.1.5 Warehouse Inventory and Maintenance

Store, organize, and inventory all Space Aggressor equipment with accurate accounting of status, location, and availability, conduct and track maintenance of Government equipment in accordance with

periodic maintenance requirements identified in AFMAN 17-1203 and conduct Government equipment inventory in accordance with AFI 23-101, Utilizing Government provided inventory software and hardware.

Performance Standards
a) Standard: The contractors will maintain an accurate accounting for USG equipment status, location and availability IAW 527 SAS SOPs with zero loss.
Deliverable
A013: Equipment Inventory Reports (monthly)
A014: Maintenance Tracking Logs

3.1.6 Education, Training, and Certification Programs

The contractor assigned to 527 Space Aggressor Squadron (527 SAS) Training Flight Shall:
Execute 527 SAS education, training, certification, and qualification programs according to Operating Instruction (OI) This includes

Space Electromagnetic Warfare Mission Qualification Training (SEW MQT), Space Electromagnetic Warfare Upgrade Training (SEW UT) Crew Chief certification, Instructor certification, following 527 SAS direction and using Government-provided courseware.

Develop and maintain courseware and curriculum aligning with the unit's current operational needs and according to the 527 Maser Task List (MTL). This includes

- Operating equipment and simulators for realistic training and evaluation scenarios.
- Demonstrating proper system setup, operation, and teardown procedures.
- Providing classroom instruction on GPS, SATCOM, and ASN missions.
- Analyzing evolving missions and recommending courseware updates.
- Training schedule and coordination
- Maintain, generating, and processing training records.

Support 527 SAS Missions, operating using SATCOM, GPS, and ASN equipment up to the qualified certified position.

Support the development and maintenance of Aggressor education, training and certification programs as outlined in 527 Space Aggressor OI Volume II and in accordance with AF Instructional System Design (ISD) AFH 36-2235 v1. This includes:

- EA and SATCOM equipment operations for training and evaluation scenarios
- Courseware materials production
- Maintaining training folders
- Demonstrating proper system setup
- Operations and tear down
- Classroom Instruction

Review, update, and maintain courseware and curriculum for 527 SAS IQT, MQT, and SME certification for GPS, SATCOM, and ASN missions.

DRAFT

Instruct initial overview of the 527 SAS mission and history, introduce Space Aggressor fundamentals (radio frequencies and signals, general adversary threats, adversary replication systems, and warehouse operations). IQT is typically one week in length.

Instruct Aggressor MQT for GPS, OW and SATCOM mission areas.

Support and assist in the development and instruction of Recurring Training (RT) as needed. RT will be conducted in accordance with 527 SAS direction with certified instructors utilizing Government provided courseware.

Review all courseware annually and provide recommendations to 527 SAS for updates and revisions.

Assist with updating and implementing approved courseware changes into Aggressor training.

Performance Standards
a) Standard: Certified/qualified contractor shall assist the 527 SAS with tasks above in line with the unit's tempo and guidance from the 527 SAS.
b) Standard: Contractors that are certified by the 527 SAS as instructors shall assist the 527 SAS in the maintenance and updating of courseware and curriculum for 527 SAS IQT, MQT, and SME certification for GPS, Cyber, On-orbit ASAT, SATCOM and ASN missions with defects or negative feedback.
Deliverable
A015: Training Courseware Materials
A016: Training Schedules
A017: Student Evaluation Reports

3.1.7 Reach-back and Surge Support

Provide reach back and surge support to in-field teams up to 100 man-hours each period of performance and on-call technical support as may be required for reach-back support. Exercise and travel constraints may require performance outside of normal duty hours as mission directed, with the Government providing notification at least 15 days prior to any support needed for reach-back and surge support and All reach-back and surge support will be at the direction of the Government and reimbursed/accounted for as part of the firm fixed price, not to exceed, Contract Line Item Number (CLIN), where any remaining funds will be deobligated to the buying activity.

Performance Standards
a) Standard: Contractor will clearly indicate when Surge/Reach back support is taking place and will provide input prior to approval if certain activities will require Surge/Reach back support. If the contractor is working within the Surge/Reach back support window they will make all efforts to minimize hours to only those required to accomplish mission.
Deliverable
A018: Reach-back Technical Support Incident Logs
A019: Equipment Inventory Reports

DRAFT

3.1.8 Exercise/Inspection Support

Provide equipment log sheets to the USG following each mission, process and perform quality control and data verification on mission data, provide the data in the format required by USG personnel or customers, and identify and report on all deficiencies associated with operations, resources and/or processes.

Performance Standards

a) Standard: Contractor will support 100% of tasked exercises while logging all equipment tasked to include strategies for maintenance and replacement for damaged items.

Deliverable

A020: Equipment Log Sheets

A021: Mission Data Quality Control Reports

A022: Deficiency Reports (Operations, Resources, Processes)

3.1.9 SATCOM and GPS

Attend exercise planning conferences and other conferences in support of topics related to planning exercises. This includes but not limited to: Deconfliction conferences, Combined Force Space Component Command, J2 (Intel) conferences, National Reconnaissance Office (NRO) Threat conferences, Space Control Working Group, etc.).

Shall qualify and maintain certification as an operator, crew chief, and instructor in both mission areas (SATCOM & GPS) as directed by 527 SAS to meet mission needs. The certification process will be administered by 527 SAS.

Provide support to event execution and periods of exercise support as required. These events/exercises may take place outside of normal day-shift hours and the contractor should flex their schedules to account for this support without incurring overtime or additional costs to the Government.

Support mission requirements as either SATCOM CCH and/or Operator up to 100 TDY days per year and with the ability to support at least two simultaneous missions.

Provide subject matter expertise for system packing, shipping, unpacking, setup, operation, troubleshooting, repair, and teardown. Packing may include pallet building for military airlift shipments and/or commercial freight.

Will instruct all mission/command allocated SATCOM & GPS utilizing 527 SAS instruction materials as a certified instructor.

Conduct research and analysis into future SATCOM & GPS EA suites and provide recommendations using a cost benefit analysis approach.

Provide instruction on SATCOM & GPS capabilities, limitations, vulnerabilities, and effects of these on the mission. Support and develop replication of threat systems employed by adversaries.

DRAFT

Provide support in maintaining SATCOM & GPS inventory to include accounting for items, identify missing items, inspection, preventative maintenance, broken components, and submit required paperwork, and follow-up/track all items until closed.

Provide support to Configuration Control Boards (CCB) with slide deck preparation, minutes, technical expertise/input, and research on estimates/analysis on buying new systems and present to CCB.

Advise and notify 527 SAS of scheduling conflicts for equipment, training, pack-out, ops testing, tours/demos, maintenance repairs, etc.

Provide support to 527 SAS for all system upgrades on hardware, software, instrumentation, and special test equipment to include design, modification, fabrication, integration, validation, and configuration documentation.

Provide support for the development of advanced methods for generating EW waveforms utilizing equipment and developed systems.

Plan the laydown of SATCOM equipment, pack, deploy, operate, perform field maintenance, and redeploy SATCOM equipment in both CONUS and OCONUS locations.

Plan the laydown of GPS EMI suites (GPS jammers, trucks, modems, generators, fuel, antennas, amplifiers, cables and various equipment listed in Appendix A). Plans shall include activities to pack, deploy, operate, perform field maintenance, and redeploy.

Support coordination of ongoing efforts and initiatives with 746th Test Squadron, 266th Range Squadron, ACC/A3 and other appropriate agencies to facilitate interoperability of GPS mission requirements.

Special Requirements:
Attain appropriate licenses/qualifications to operate forklifts and pallet jacks for the equipment listed in Appendix A.
Capable of performing a two-person lift of at least 100 lbs. (50 lbs. per person).

<u>Performance Standards</u>
a) Standard: The contractor shall be capable of travelling with Aggressor crews to exercise locations (sometimes remote locations) to act as CCHs or operators for these operations. 100% of tasked exercises are supported with present-for-duty and certified CCHs or operators.
b) Standard: The contractor shall support development of Aggressor participation in synthetic environments, where such participation is requested by the exercise planning team. 100% of tasked exercises are supported with present-for-duty and certified threat analysts. No negative feedback from supported agencies regarding contractor performance.
<u>Deliverable</u>
A023: SATCOM/GPS Equipment Status Reports
A024: Exercise Participation Reports (TDY days, CCH/Operator roles)

DRAFT

A025: System Upgrade Reports

3.2 Space Aggressor OW Support

3.2.1 Instruction and Training

Provide comprehensive instruction in both RPO Mission Planning and Space Battle Management, including delivering a minimum of 40 hours of instruction for each subject annually. Crucially, the RPO Mission Planning instruction must be highly effective, with post-training evaluations demonstrating that at least 90% of attendees found the instruction as either "effective" or "highly effective." Similarly, the Space Battle Management instruction must incorporate realistic adversary tactics, techniques, and procedures (TTPs) and be directly relevant to current operational scenarios, ensuring trainees are prepared for real-world challenges. The contractor will conduct OW (Orbital Warfare) operator training utilizing provided modeling and simulation systems with a target of at least 80% achieving certification as OW operators upon program completion and maintain their own valid certifications as both an OW operator and instructor.

Performance Standards

a) Standard: Deliver a minimum of 40 hours of RPO mission planning instruction annually. Post-training evaluations shall indicate that at least 90% of attendees found the instruction "effective" or "highly effective".

b) Standard: Deliver a minimum of 40 hours of Space Battle Management instruction annually.

c) Standard: At least 80% of trainees shall achieve certification as OW operators upon completion of the training program.

d) Standard: Maintain valid certifications as an OW operator and instructor.

Deliverable

B001: RPO Mission Planning Training Materials

B002: Space Battle Management Training Materials

B003: OW Operator Training Certification Rates

3.2.2 Future Work Option

3.2.2.1 Curriculum Maintenance and Development

Comprehensive oversight of the unit's Orbital Warfare training curriculum and courseware, encompassing an annual review to ensure the accuracy, currency, and accessibility of all materials. Any necessary updates identified during the review must be completed within 30 days, with all changes requiring approval from unit leadership. Updated courseware documentation should be meticulously submitted, including tracked changes and a clear rationale for each modification. The contractor is tasked with maintaining the courseware by implementing approved updates and revisions within 15 days of approval and adapting the curriculum to reflect the evolving threat landscape and adversary TTPs.

Performance Standards

a) Standard: Review 100% of existing unit OW curriculum and courseware annually. All updates shall be completed within 30 days of identification of needed changes and approved by 57 SAS leadership.

DRAFT

Implement 100% of approved updates and revisions to OW courseware within 15 days of approval.
Incorporate realistic adversary TTPs into the curriculum within 60 days of updated intelligence assessments.
Deliverable
BF01: OW Curriculum and Courseware Update Documentation

3.2.2.2 –Weapons and Tactics Training, Integration, and CONOPS Support

The contractor shall support the Orbital Warfare Aggressors Weapons and Tactics (W&T) shop by delivering instruction, standards enforcement, tactics development, and community integration in direct support of US Space Force (USSF) training and operational readiness. The contractor's efforts shall focus on mission planning and debrief, tactics development, aggressor threat replication, and advanced training delivery. All work will directly enhance unit lethality, credibility, and tactical proficiency. Contractor will:

Instruct mission planning and debriefing education and training for unit personnel, ensuring alignment with established USSF and unit standards.
Enforce debrief standards across the unit and maintain a centralized lessons learned repository to capture, curate, and disseminate tactical insights.
Lead the unit's tactics development program, to include authorship, revision, and sustainment of tactics reference materials.
Develop and conduct advanced training events for unit personnel, focusing on tactics employment, adversary replication, and operational/tactical problem-solving.
Review mission qualification training products for accuracy, completeness, and tactical relevance, providing recommendations for improvement as required.
Support development and sustainment of an aggressor threat replication guide in coordination with the intelligence shop, ensuring threat realism and fidelity.
Integrate with the broader USSF and joint space community through exercise support, mobile teach teams, and external engagement events.

Performance Standards
a) Standard: Deliver mission planning and debriefing instruction in accordance with unit standards and training objectives. Instruction shall be assessed as effective by unit leadership and trainees.
b) Standard: Enforce debrief standards during training and operational events and maintain a current, accessible lessons learned library updated throughout the year.
c) Standard: Lead and sustain a tactics development program, ensuring tactics references are accurate, current, and reflective of unit employment and adversary capabilities.
d) Standard: Plan and conduct advanced training events that address identified training gaps and enhance tactical proficiency beyond mission qualification training.
e) Standard: Review MQT materials and events for accuracy, completeness, and tactical relevance, providing documented feedback to unit leadership.
f) Standard: Collaborate with the intelligence shop to develop and maintain an aggressor threat replication guide that accurately reflects adversary capabilities and employment.
g) Standard: Support exercises and mobile teach teams, integrating unit tactics and aggressor expertise with the broader operational community.

Deliverables
BF02: Mission Planning and Debrief Instruction Materials and Support
BF03: Debrief Standards Enforcement and Lessons Learned Repository
BF04: Tactics Development Products and Tactics Reference Library
BF05: Advanced Training Plans and Training Assessment Reports
BF06: Mission Qualification Training Review Assessments
BF07: Aggressor Threat Replication Guide (in coordination with Intelligence)
BF08: Exercise and Mobile Teach Team Support Products and Instruction

3.2.2.3 Operations and Exercise Support

Provide comprehensive support for Aggressor participation in synthetic environment exercises, including scenario development, system configuration, and real-time support, and extensive operational and technical support to the USSF, including acting as certified operators for all tasked exercises. They will provide operational support as an OW operator and coordinate with external agencies, conduct annual research and cost-benefit analysis on future OW suites, and develop/maintain OW aggressor training materials quarterly based on the latest intelligence. Furthermore, the contractor is responsible for comprehensive conference planning, on-site support resolving issues within one-hour, post-conference reporting within 30 days, and developing briefing materials at least two weeks in advance.

Performance Standards

a) Standard: Provide operational support as an OW operator, as requested by leadership, up to 100 TDY days per year.
b) Standard: Act as certified operators for 100% of tasked exercises.
c) Standard: Coordination activities shall be documented in monthly reports.
d) Standard: Advise and notify USSF of scheduling conflicts for personnel availability for OW missions, exercises, and training within 24 hours of identification.
e) Standard: Conduct research and analysis into future OW suites and provide a comprehensive cost-benefit analysis annually.
f) Standard: Develop a comprehensive conference plan at least 90 days prior to each conference.
g) Standard: Any issues that arise shall be resolved within 1 hour.
h) Standard: Prepare a post-conference report within 30 days of each conference.
i) Standard: Develop briefing material for conference attendees and conference presenters at least 2 weeks before the conference.
j) Standard: The contractor shall be capable of travelling with Aggressor crews to event locations (sometimes remote locations) to act as CCHs or operators for these operations. 100% of tasked exercises are supported with present-for-duty and certified operators.
k) Standard: Support Aggressor participation in synthetic environment exercises requested by the exercise planning team.
l) Standard: Update and maintain OW aggressor training, products, capabilities, and simulation environments quarterly, based on latest intelligence assessments of adversary capabilities.
m) Standard: The contractor shall support development of Aggressor participation in synthetic environments, where such participation is requested by the exercise planning team. 100% of tasked exercises are supported with present-for-duty and certified threat analysts. No negative feedback from supported agencies regarding contractor performance.

DRAFT

Deliverable
BF09: OW Operator Support Reports (TDY days, Exercise Participation)
BF10: Future OW Suite Cost-Benefit Analysis
BF11: Conference Plans
BF12: Post-Conference Reports

3.2.2.4 **Intelligence Analysis Support**
The contractor shall Research and network system subject matter on intelligence community Information Systems (IS), (i.e. Joint Worldwide Intelligence Communications System (JWICS)) to create and present briefings and white papers to Air, Space, and Cyberspace operations professionals. Create and present weekly classified intelligence briefs focused on space and space control activities conducted by U.S. adversaries over the period of interest. The briefings shall include a technical analysis of the tactics, system, and operator proficiency demonstrated by the adversary during the observed operation. 527 SAS will provide slide format to be utilized for content. Provide intelligence briefings, instruction, and advisory support to various training for SAS operators and external customers. This shall include specific threat briefings that are tailored to a specific training audience and their system.
Support exercise planning for Master Scenario Event List builds for threats to be injected into training with modeling and simulation. Travel may be required and will be conducted in accordance with PWS para 2.5.
Maintain a database of observed adversary TTPs, and mission systems to support creation and validation of Space Aggressor tactics. SIPR and/or JWICS will be utilized as the repository for this database. These TTPs shall be updated in the Space Aggressor Adversary Threat Replication Guide (ATRG) and space threats brief quarterly.
Support the evaluation of new military systems and commercially available technologies for the potential threat(s) they may present to U.S./Allied forces. Travel may be required and will be conducted in accordance with PWS para 2.5.
Support threat intelligence community conferences, cross-talks, and Weapons School (Delta 1) syllabus reviews.
Develop/recommend implementation plans for applying intelligence information and procedures to SAS projects to support military training and exercises.
Attend conferences for exercise planning as requested by the Government. Examples include: Deconfliction Conferences, Combined Force Space Component Command, J2 (Intelligence) conferences, NRO Threat Conferences, Space Control Working Group, etc.). Notify the Government COR of scheduling conflicts for personnel to support missions/exercises/training as needed.

Performance Standards
a) Standard: The Current Intelligence Briefings shall include a technical analysis of the tactics, system, and operator proficiency demonstrated by the adversary during the observed operation IAW unit requirements and Intel Flight SOI.
b) Standard: Weekly CIB created and presented 90% of the time.
Deliverable
BF13: Weekly Classified Intelligence Briefings on Adversary Space Activities

BF14: Tailored Threat Assessments for Specific Training Audiences

3.3 Space Cyber Range Support

3.3.1 Intelligence and Threat Analysis Support
Provide actionable Intelligence and Threat Analysis Support, integrating threat-based intelligence with cyber aggressor operations to ensure realistic and current threat representation in training and operational scenarios. The contractor will conduct in-depth, integrated cyber intelligence analysis, combining data from multiple sources to provide a comprehensive understanding of the cyber threat landscape relevant to USSF operations. They will also support threat-based requirements development for USSF operations, serve as subject matter expert, and develop tailored intelligence products, such as threat assessments, briefings, and analytical reports, to support specific USSF operational requirements. They will need to create and maintain a usable database of adversary TTPs, sophistication level, current/future intent, capable TTPs, tools, and classification of each item. Database will also provide USSF systems, areas of mission coverage, TTPs, hardware/software, and include vulnerabilities. Prefer for contractor to have accomplished the Joint Cyber Analysis Course.

Performance Standards
Standard: Cyber intelligence analysis reports will be delivered within 48 hours of request.
Standard: Cyber Intelligence Analysis reports should include technical analysis of the tactics, systems and operator proficiency demonstrated by the adversary
Standard: Tailored intelligence products will receive an average score of at least 7 out of 10 on a government evaluation of quality and relevance.
Deliverable
C001: Cyber Intelligence Analysis Reports
C002: Threat-Based Requirements Documents
C003: Tailored Intelligence Products

3.3.2 Red Team Technical Expertise
Provide qualified Red Team Technical Leadership by using and implementing tools, tactics and procedures consistent with cyber adversaries. Contractor should have knowledge of risk management protocols, network infrastructure, reporting, and cybersecurity. The Technical Lead (TL) serves as the primary technical authority for all network operations and mission execution activities, reporting to the Mission Commander/Crew Commander (MC/CC) and overseeing technical aspects of red team operations. Technical Leads will need to participant in Cyber Exercises to demonstrate realistic Red Team capabilities. TLs will assist in mentoring and providing on-the-job training to junior Red Team members.

Performance Standards
a) Standard: All network actions will be conducted in accordance with established Risk Management (RM) protocols as approved by USSF cybersecurity leadership.
b) Standard: Maintain a CREST Certified Red Team Specialist, CISSP, GPEN or equivalent certification
Deliverable

DRAFT

C004: Mission Reports and Briefings

3.3.3 Future Work Option

3.3.3.1 Cyber Range Operations and Training Coordinator
Design, Develop, and Execute Cyber Range and Aggressor Training Programs. Create and Review Cyber Range and Aggressor Training Materials, Analyze Trainee Performance in Cyber Range Exercises. The contractor will play a pivotal role in ensuring personnel are adequately trained and certified to operate effectively within the cyber range environment and during real-world offensive and defensive cyber operations and will be responsible for the development and maintenance of Master Training Lists (MTL) that comprehensively address the specific execution needs and training requirements of all supported units. The contractor will need to coordinate with Intel and weapons and tactics to incorporate up to date TTPs into the training plan.

Performance Standards
a) Standard: A MTL will be created and maintained to satisfy the training needs of both Range and Aggressor workforce
b) Standard: Deploy a training plan that covers job qualification standards and specific work center tasks for both Cyber Range and Aggressor members.
c) Standard: Training materials will be reviewed and updated at least quarterly to reflect current threats and best practices, as documented in version control logs.
Deliverable
CF01: Cyber Range and Aggressor Training Programs
CF02: Training Materials
CF03: Trainee Performance Reports

3.3.3.2 Cyber Weapons & Tactics Support
The contractor shall maintain up-to-date documentation of adversary and U.S. DoD mission systems and architectures based on current intelligence, developing comprehensive adversarial emulation plans for realistic exercises and operations. This includes developing, updating, and managing a repository of tools, exploits, and malware that emulate adversarial TTPs, ensuring they are functional, secure, and used in compliance with applicable regulations. Additionally, the contractor will develop and maintain procurement lists for necessary tools and exploits from approved DoD sources, justifying requests and managing the inventory effectively.

Performance Standards:
Adversarial Emulation Effectiveness: Adversary emulation plans, tools, and capabilities will be generated based off of intel and will be created/acquired to mission planning needs.
Tool and Capability Functionality: Tools, exploits, and malware developed shall be validated to function as intended and effectively emulate adversarial TTPs.
Compliance with Policies and Regulations: All tools, exploits, and malware shall be developed and used in compliance with applicable laws, regulations, and DoD policies.
Deliverable
CF04: Adversarial Emulation Plans: Detailed plans for adversarial emulation exercises and operations.

DRAFT

CF05: Cyber Weapons and Tools Repository: A repository of developed and procured cyber weapons, tools, exploits, and malware.

3.3.3.3 Range Infrastructure Specialist
Design, build, and maintain cyber range infrastructure, ensure cyber range operational readiness, ensure a secure, reliable, and scalable cyber range environment, integrate cloud services for cyber range functionality and optimize cyber range performance. They will also ensure all IT systems meet unit and mission requirements while maintaining operational readiness, with a particular focus on aligning system architectures with cyber range capabilities and 33 RGS operational needs, ensuring that the 33 RGS's IT infrastructure is optimized for seamless interaction with the range environment and effectively supports the 33 RGS mission.

Performance Standards
a) Standard: The cyber range infrastructure will maintain an uptime of at least 95% per month, as measured by automated monitoring systems.
b) Standard: Security vulnerabilities will be identified and remediated within 48 hours of detection, as evidenced by closed vulnerability tickets.
Deliverable
CF06: Infrastructure Design Documents
CF07: Uptime Reports
CF08: Security Vulnerability Reports

3.3.3.4 Cyber Range Engineering Support
The contractor will ensure the secure configuration, operation, and monitoring of the cyber range environment, utilizing offensive security insights to proactively identify and mitigate vulnerabilities in simulated environments. This role focuses on bolstering an organization's cybersecurity posture. The contractor will need to validate security controls, assess network architectures against simulated attacks, and ensure compliance with relevant security policies and standards. The contractor will work closely with infrastructure and intel to understand potential attack vectors and translate those into proactive security measures and configurations.

The contractor will be responsible for the security and integrity of the cyber range environment, ensuring it remains a realistic and secure platform. This includes implementing and maintaining security controls, conducting vulnerability assessments, managing security documentation, and collaborating with other team members to enhance the overall security posture of both the unclassified cyber range and classified environments.

Performance Standards
a) Standard: Development of Cyber Range security plan according to the NIST Cybersecurity Framework
b) Standard: The cyber range environment will maintain an up-time of at least 90% per month, as measured by automated monitoring systems.
Deliverable
CF09: Vulnerability Assessment Reports

DRAFT

3.3.3.5 Range Integration Specialist
Represent the interests of the 33d Range & Aggressor Squadron (33 RGS) in Cyber Range Project Planning, advocate for 33 RGS Requirements, translate the strategic vision into actionable requirements, communicate 33 RGS priorities to OTTI and identify and communicate project risks.

Performance Standards
a) Standard: The 33 RGS will be represented at 90% of cyber range project planning meetings, as evidenced by attendance logs.
b) Standard: 33 RGS requirements will be documented and communicated to OTTI within 5 duty days of identification, as evidenced by dated requirements documents submitted to OTTI.
c) Standard: Project risks will be identified and communicated to relevant stakeholders within 2 duty days of detection, as evidenced by dated risk assessment reports.
Deliverable
CF10: Meeting Minutes
CF11: Requirements Documents
CF12: Risk Assessment Reports

3.3.3.6 Cyber Stan/Eval
Develop and maintain Red Team operational standards and evaluation criteria, conduct Red Team personnel evaluations, certify Red Team Operators, maintain Red Team evaluation documentation and provide feedback and recommendations for Red Team improvement. They will ensure that all aggressor training and operations meet or exceed established standards of performance, developing and implementing quality assurance measures specifically tailored to red team activities, ensuring that deliverables meet or exceed government specifications and requirements for realistic and effective adversary emulation.

Performance Standards
a) Standard: Red Team operational standards and evaluation criteria will be reviewed and updated at least annually as evidenced by dated revision logs.
b) Standard: Red Team personnel evaluations will be conducted within 120 days of assignment to the 33 RGS or annually as evidenced by completed evaluation forms submitted to 33 RGS leadership.
Deliverable
CF13: Red Team Operational Standards and Evaluation Criteria
CF14: Personnel Evaluation Reports
CF15: Red Team Certification Database

3.3.3.7 Cyber Planner
Coordinate to design, develop, and document realistic and complex cyber range scenarios that simulate cyberattacks against space systems and other critical infrastructure. This includes integrating current threat intelligence to replicate threat actor tactics, techniques, and procedures (TTPs) and developing comprehensive scenario documentation, including detailed timelines, injects (simulated events), and participant instructions. The Cyber Planner will collaborate to configure cyber range infrastructure to support exercise scenarios, and collaborate with subject matter experts (SMEs) in

DRAFT

cybersecurity, intelligence, and space operations to develop realistic and challenging exercise scenarios that push trainees to adapt and improve their skills. The cyber planner will also be responsible for collecting and analyzing data from cyber range exercises to identify areas for improvement in training and security posture, and creating after-action reports (AARs) summarizing exercise results, identifying key findings, and recommending actionable corrective measures.

Performance Standards
a) Standard: Cyber range scenarios will be designed in coordination with Cyber Squadron ops tempo and documented with exercise timelines, participant roles and objectives
b) Standard: Threat intelligence will be integrated into all cyber range scenarios and documented by a threat assessment table included with scenario information.
c) Standard: After-action reports will be delivered within 2 weeks of exercise completion with clearly defined key findings, trends and recommendations for corrective action.
Deliverable
CF16: Cyber Range Scenarios
CF17: Scenario Documentation
CF18: After-Action Reports

3.3.3.8 Cyber Team Chief
Provide effective leadership and oversight of cyber aggressor teams, ensuring mission readiness, coordination, and compliance. The Team Chief must ensure all activities are conducted in accordance with applicable regulations and guidelines. The contractor is required to manage and oversee cyber aggressor teams, providing guidance and direction, ensure mission readiness of all team members, verifying qualifications and training, Coordinate with stakeholders, including authorizing officials, supported units, and external entities and enforce adherence to Rules of Engagement (ROE), USCYBERCOM Standing Ground Rules (SGRs).

Performance Standards
a) Standard: Cyber aggressor teams will be managed and overseen in accordance with established policies and procedures with a review performed every 180 days with the government team.
b) Standard: All team members will meet or exceed required qualifications and training standards and have documentation on file.
c) Standard: Stakeholders will be coordinated with effectively and in a timely manner. Verify responses to all requests within 48 hours or less.
Deliverable
CF19: Team Management Plans

3.3.3.9 Cyber Operator
Execute cyber operations according to tactical plans, implementing on-network/mission system effects under the direction of the Team Chief. The Cyber Operator is responsible for the hands-on execution of cyber operations, utilizing a wide range of tools and techniques to achieve mission objectives while adhering to established guidelines and security protocols. They will participate as OPFOR in cyber exercises providing realistic cyber effects. They will configure and operate assigned tools and capabilities proficiently, analyze malware samples, conduct vulnerability assessments, and exploit

DRAFT

vulnerabilities to gain access to target systems. Throughout all operations, the Cyber Operator will maintain detailed activity logs, report anomalies, participate in mission planning and debriefing sessions, contribute to the development and improvement of operational procedures, and maintain a strong understanding of the current threat landscape and adversary TTPs.

Performance Standards
a) Standard: Cyber operations will be executed in accordance with the tactical plan and under the direction of the Team Chief with no deviations from outlined procedures.
b) Standard: Rules of Engagement (ROE), USCYBERCOM Standing Ground Rules (SGRs), and other relevant guidance will be adhered to at all times. Confirmed annual training to all.
Deliverable
CF20: Cyber Operation Execution Logs

3.4 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.

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.

3.4.1 Transition Phase-In

Contractor shall provide a Phase-In Plan. During the phase-in period, the Contractor shall provide (at a minimum) weekly briefings to the COR, the CO and the Government PM discussing problems encountered in accomplishing the phase-in, categorized as minor or major issues, progress-to-date, with schedule updates to reflect the actual progress, any variances from the phase-in plan, work-around plans being implemented to resolve problems, and clearly identify any support needed from the Government. An initial inventory of equipment, as identified in paragraph 2.10 and 3 of this PWS shall be conducted during the phase-in period within the 30 calendar days prior to the start of contract performance. Participants in this inventory shall include both the incoming Contractor, the outgoing Contractor, and the COR.

Performance Standards:

STD #1: The contractor shall obtain security clearances, Common Access Cards (CACs) and satisfy training requirements. The contractor shall implement the proposed Phase-In Transition Plan. The contractor shall shadow the incumbent service provider/contractor employees and observe duties and responsibilities.

3.4.2 Transition Phase-Out

The Contractor shall fully support and cooperate with the successor to ensure a smooth transition of all services identified in the PWS. The Contractor shall develop a Phase-Out Plan to ensure a smooth

DRAFT

transition of all on-going activities as described within this PWS. The Contractor shall conduct a physical inventory with the Government of all Government owned equipment and software with 100 percent accountability of all equipment six months prior to contract end. The contractor shall conduct another inventory with the awarded contractor prior to the equipment move to the awarded contractors training facility.

Performance Standards:

STD #1: The Contractor shall retrieve and return to the 527 SAS Security Manager all identification media, including common access cards (CAC) and restricted area badges (RAB) from contract employees that depart for any reason before the contract expires or upon termination of the contract. The Contractor shall notify the Government within 24-hours when unable to retrieve identification media from contract employees.

3.5 Associate Contractor Agreements (ACA)

Upon contract award for follow-on support, if the incumbent is not selected, the Contractor shall enter into Associate Contractor Agreements (ACA) for any portion of the contract requiring joint participation in the accomplishment of the Government's requirement.

The agreements shall include the basis for sharing information, data, technical knowledge, expertise, resources, or any combination thereof, which shall ensure the greatest degree of cooperation for the development of the program to meet the terms of the contract.

The ACA shall:

1. Identify the associate contractors and their relationships.
2. Identify the program involved and the relevant Government contracts of the associate contractors.
3. Describe the associate contractor interfaces by general subject matter.
4. Specify the categories of information to be exchanged or support to be provided.
5. Include the expiration date (or event) of the ACA.
6. Identify potential conflicts between relevant Government contracts and the ACA and include agreements on protection of proprietary data and restrictions on employees
7. A copy of such agreement shall be provided to the PCO for review before execution of the document by the cooperating contracts.

The Contractor is not relieved of any contract requirements or entitled to any adjustments to the contract terms because of a failure to resolve a disagreement with an associate contractor. However, the Government may assist the Contractor in the event of non-responsiveness from an associate contractor.

Liability for the improper disclosure of any proprietary data contained in or referenced by any agreement shall rest with the parties to the agreement, and not the Government.

All costs associated with the agreements are included in the negotiated cost of this contract. Agreements may be amended and associate contractors added or deleted as required by the Government during the performance of this contract.

DRAFT

3.6 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.

Deliverable
AA05: Meeting and Review Minutes

3.6.1 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 (content, due date), as well as key personnel roles and responsibilities.

Commented [JT12]: DID: DI-MGMT-81605
The Govt PM should also brief roles and responsibilities, CPAR, authorities.

Deliverable
AA06: Kick-Off Meeting

3.6.2 Program Management Review (PMR)

The Contractor shall present a PMR to the Government to describe cost, schedule, and performance requirements on a(n) annual basis.

Commented [JT13]: DID: DI-MGMT-81605

Deliverable
AA07: Program Management Review

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**
Department of Defense (DoD) Instructions/Manuals			
D/G	**Pub Number**	**Title**	**Date**
G	DoDM 5200.01 Vol 3	DoD Information Security Program: Protection Of Classified Information	11 Apr 2022
G		National Industrial Security Program	21-Dec-22

	32 CFR Part 117 DoDM	Operating Manual	
G	DoDI 5220.22_Vol 2	National Industrial Security Program: Industrial Security Procedures for Government Activities	20-Feb-25
G	DoDIM5200.01 V1	Information Security Program: Overview, Classification and Declassification	17-Jan-25
G	DoDIO-2000.16V1	Antiterrorism (AT) Program Implementation	06 Dec 2020
G	DoDM 5200.02	DoD Personnel Security Program	29-Oct-20
G	DoDM 5205.07	Special Access Program (SAP) Security Manual: Personnel Security	17-Jan-25
G	32 CFR Part 117	National Industrial Security Program	21-Dec-20
G	DoDMAN 5200.2	Personnel Security Program	29-Oct-20

Air Force Instructions/Manuals			
D/G	**Pub Number**	**Title**	**Date**
G	AFMAN 14-403	Sensitive Compartmented Information Security and Intelligence, Surveillance, and Reconnaissance Systems Cybersecurity and Governance	02 Sep 2019
G	AFMAN 17-1203	Information Technology (IT) Asset Management (ITAM)	17 May 2018
G	AFMAN 17-1302-O	Communications Security (COMSEC) Operations	13-Dec-24
G	AFMAN 24-306	Operation of Air Force Government Motor Vehicles	29 Jul 2020
G	AFMAN 32-7002	Environmental Compliance and Pollution Prevention	03 Feb 2020
G	AFMAN 91-203	Air Force Occupational Safety, Fire and Health Standards	10 Dec 2018

Technical Orders			
D/G	**Pub Number**	**Title**	**Date**
G	319 CTS CDG	Course Curriculum Guide	18 Mar 2021

DRAFT

G	319 CTS OI 36-2203	319 CTS Operations	22 Feb 2020
G	AFI 10-701	Operations Security	09 Jun 2020
G	DAFMAN 16-201	Air Force Foreign Disclosure and Transfer Program.	19-Jan-21

Misc Publications			
D/G	**Pub Number**	**Title**	**Date**
D	CJCSM 3212.03A	Performing Tests, Training, and Exercises Impacting the Global Positioning System (GPS) in the United States and Canada	8 Nov 2019
G	CJCSI 3320.01D	Joint Electromagnetic Spectrum Operations (JEMSO)	24-Jan-25
G	18--AFPD 17-1	Information Dominance Governance and Management	12 Apr 2016
G	4407 Spec Analyzer	User's Guide Agilent Technologies ESA Series Spectrum Analyzers	Dec 2006
G	ICD 705	Physical and Technical Security Standards for Compartmented Information Facilities	17-Sep-10
G	N9340B	Agilent N9340B Handheld Spectrum Analyzer	Jul 2009
G	N9344	Agilent N9342C/43C/44C Handheld Spectrum Analyzer	Sep 2005
G	PR100	R&S PR100 Portable Receiver Manual	2014
G	Rhode and Schwarz FSVA	R&S FSVA/FSV Signal and Spectrum Analyzer Operating Manual	2016
G	SLM-5650A	Satellite Modem Installation and Operation Manual	2012
G		USSF Cyberspace Roadmap and Implementation Plan 20210806	
G		USSF PPLAN to CS-I PAD D15-03	
G		CS-I PAD D15-03	

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.

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

DRAFT

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				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
AA01	Monthly Status Report (MSR)	2.2	Monthly	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 - Major tasks/activity status - 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				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
AA02	Contractor Personnel Roster	2.2.4	Monthly	COR PCO
Description: Roster of all current personnel with an indicator of which require and possess a CAC or access badge and status of NDA completion.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
AA03	Travel Report	2.5	Within 10 business days from travel.	COR PCO

DRAFT

Description: For all trips, the Contractor shall provide a trip report within ten (10) business days of the return date from travel. Extensions may be granted by the COR on a case-by-case basis. As a minimum, trip reports will include the objectives and outcomes of the trip. Trip reports do not have a specific format and may range from an email to a formal presentation depending on the type of trip.

Identifier	Name	PWS #	Schedule	Distribution
AA04	Non-Disclosure Agreement	2.6.6	Within 5 days of starting on the contract.	COR PCO

Description: 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.

Identifier	Name	PWS #	Schedule	Distribution
AA05	Meeting and Review Minutes	3.6	2 weeks following meeting/review	COR PCO

Description: Minutes from the meeting or review.

Identifier	Name	PWS #	Schedule	Distribution
AA06	Kick-Off Meeting	3.6.1	NLT 10 days after start	COR Units Required

Description: 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 (content, due date), as well as key personnel roles and responsibilities.

Identifier	Name	PWS #	Schedule	Distribution
AA07	Program Management Review	3.6.2	Annual	COR PCO

Description: The Contractor shall present a PMR to the Government to describe cost, schedule, and performance requirements on a(n) annual basis.

Deliverable Table				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**

DRAFT

A001	Weekly Classified Intelligence Briefings on Adversary Space Activities	3.1.1	Weekly	COR
Description: The slide deck and supporting materials for the weekly classified intelligence briefing, including technical analysis of adversary tactics, system, and operator proficiency.				

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
A002	Tailored Threat Assessments for Specific Training Audiences	3.1.1	As required, NLT 15 days prior to the supported training event.	COR
Description: A specific threat assessment and briefing package tailored to the training audience and their systems, based on the latest intelligence.				

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
A003	Exercise Approval Packages (CAAPs, EA Requests, etc.)	3.1.2	As required.	COR
Description: Completed and staffed exercise approval packages, including but not limited to CAAPs, GPS EA Requests, DSRs, and Satellite Access Requests, ready for government review and submission.				

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
A004	Operations Requests (ORs)	3.1.2	As required.	COR
Description: Completed Operations Requests (ORs) and Range Request Forms (RRFs) drafted for government review and submission to the appropriate range organization.				

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
A005	Operations Directives (ODs) Review Reports	3.1.2	Within 3 business days of OD publication.	COR
Description: A report or email summarizing the review of published Operations Directives, highlighting any discrepancies, errors, or potential conflicts with Aggressor requirements and resources.				

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
A006	Aggressor CONOPS Documents	3.1.3	As required.	COR

DRAFT

Description: Documentation detailing the Concept of Operations (CONOPS) for replicating adversary threats against space systems.

Identifier	Name	PWS #	Schedule	Distribution
A007	Adversary TTPs Database Updates	3.1.3	Quarterly	COR

Description: A report or direct entry log confirming that the database of adversary Tactics, Techniques, and Procedures (TTPs) has been updated with the latest intelligence.

Identifier	Name	PWS #	Schedule	Distribution
A008	Implementation Plans for Applying Intelligence	3.1.3	As required.	COR

Description: A plan detailing the recommended implementation of new intelligence information and procedures into SAS projects, training, and exercises.

Identifier	Name	PWS #	Schedule	Distribution
A009	Commercial Off-the-Shelf Component Procurement Reports	3.1.3	As required.	COR

Description: A report detailing research on COTS components, including availability, cost, and procurement recommendations to create or upgrade squadron systems.

Identifier	Name	PWS #	Schedule	Distribution
A010	PMI/PDI Reports	3.1.4	Within 5 business days of system return or completion of maintenance.	COR

Description: A report detailing the results of Periodic Maintenance Inspections (PMI) or Post-Deployment Inspections (PDI), including mission capability (MISCAP) assessment, troubleshooting results, and recommendations for parts and repairs.

Identifier	Name	PWS #	Schedule	Distribution
A011		3.1.4	As required.	COR

DRAFT

	Equipment Packing and Shipping Documentation			

Description: All necessary documentation for the packing and shipment of mission equipment, including packing lists, pallet build diagrams, and shipping forms.

Identifier	Name	PWS #	Schedule	Distribution
A012	Reach-back Technical Support Incident Logs	3.1.4	Monthly	COR

Description: A log of all instances of reach-back technical support provided to deployed forces, detailing the issue, support provided, and resolution.

Identifier	Name	PWS #	Schedule	Distribution
A013	Equipment Inventory Reports	3.1.5	Monthly	COR

Description: A detailed report of all Space Aggressor equipment, accounting for status, location, and availability, verified against the government-provided inventory system.

Identifier	Name	PWS #	Schedule	Distribution
A014	Maintenance Tracking Logs	3.1.5	Updated continuously; status report provided monthly.	COR

Description: A log tracking all periodic and corrective maintenance performed on government equipment, IAW AFMAN 17-1203.

Identifier	Name	PWS #	Schedule	Distribution
A015	Training Courseware Materials	3.1.6	Annually, or as required for new course development.	COR

Description: All instructor and student materials for IQT, MQT, and certification programs. Submitted upon initial development and after annual reviews/updates.

Identifier	Name	PWS #	Schedule	Distribution
A016	Training Schedules	3.1.6		COR

DRAFT

			Monthly, or as training events are planned.	

Description: A schedule of all planned training events, including IQT, MQT, and Recurring Training (RT), coordinated with unit requirements.

Identifier	Name	PWS #	Schedule	Distribution
A017	Student Evaluation Reports	3.1.6	Within 5 business days of course completion.	COR

Description: A report summarizing student performance, evaluation results, and certification status following the completion of a training course.

Identifier	Name	PWS #	Schedule	Distribution
A018	Reach-back Technical Support Incident Logs	3.1.7	Monthly	COR

Description: A log detailing all instances of reach-back and surge support provided, including man-hours expended, the nature of the support, and the resolution.

Identifier	Name	PWS #	Schedule	Distribution
A019	Equipment Inventory Reports	3.1.7	Monthly	COR

Description: A detailed inventory report of all Space Aggressor equipment, accounting for status, location, and availability, submitted as part of the monthly reporting cycle.

Identifier	Name	PWS #	Schedule	Distribution
A020	Equipment Log Sheets	3.1.8	Within 3 business days following each mission/exercise.	COR

Description: Completed log sheets for all equipment used during a mission or exercise, detailing usage and any issues encountered.

Identifier	Name	PWS #	Schedule	Distribution
A021	Mission Data Quality Control Reports	3.1.8		COR

			Within 5 business days following each mission/exercise.	
Description: A report summarizing the quality control and data verification performed on mission data, formatted as required by the customer.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
A022	Deficiency Reports (Operations, Resources, Processes)	3.1.8	As required, included in monthly status report.	COR
Description: A report identifying any deficiencies found in operations, resources, or processes, including analysis and recommendations for correction.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
A023	SATCOM/GPS Equipment Status Reports	3.1.9	Monthly	COR
Description: A monthly report detailing the inventory and status of all SATCOM & GPS equipment, including operational readiness, missing items, and status of maintenance actions.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
A024	Exercise Participation Reports (TDY days, CCH/Operator roles)	3.1.9	Monthly	COR
Description: A monthly summary of exercise participation, detailing TDY days used, missions supported, and roles filled (e.g., SATCOM CCH, GPS Operator).				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
A025	System Upgrade Reports	3.1.9	As required	COR
Description: A report detailing support provided for system upgrades, including design, modification, integration, validation, and configuration documentation.				

Deliverable Table
[redacted]

DRAFT

Identifier	Name	PWS #	Schedule	Distribution
B001	RPO Mission Planning Training Materials	3.2.1	Annually, 30 days prior to the start of instruction.	COR
Description: All training materials, including presentation slides, lesson plans, and practical exercises, required to deliver the RPO Mission Planning instruction.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
B002	Space Battle Management Training Materials	3.2.1	Annually, 30 days prior to the start of instruction.	COR
Description: All training materials, including presentation slides, lesson plans, and scenario-based exercises, required to deliver the Space Battle Management instruction, incorporating the latest adversary TTPs.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
B003	OW Operator Training Certification Rates	3.2.1	Quarterly	COR
Description: A report detailing the number of trainees who attended the OW operator training and the percentage who successfully achieved certification during the reporting period.				
FUTURE WORK				
Deliverable Table				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF01	OW Curriculum and Courseware Update Documentation	3.2.2.1	Annually	COR
Description: Documentation of the annual review of all OW curriculum and courseware. Includes a summary of findings, tracked changes for all modifications, and the rationale for each update.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF02	Mission Planning and Debrief Instruction Materials and Support	3.2.2.2	As requested	COR
Description: All materials needed for instruction, such as presentation slides, lesson plans, and practical exercises for mission planning and debriefing. Includes support provided during training events.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**

BF03	Debrief Standards Enforcement and Lessons Learned Repository	3.2.2.2	Updated continuously; status report provided quarterly.	COR
Description: An accessible repository or database of lessons learned from training and operational events. Includes documentation of debrief standards enforcement actions.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF04	Tactics Development Products and Tactics Reference Library	3.2.2.2	Updated as new tactics are developed; a summary of updates is provided quarterly.	COR
Description: All developed tactics documents, TTPs, and reference materials. Includes the maintained library/repository of these products.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF05	Advanced Training Plans and Training Assessment Reports	3.2.2.2	Plan due 30 days prior to the event; Assessment report due 14 days after event completion.	COR
Description: Comprehensive plans for each advanced training event and post-event assessment reports detailing training effectiveness, participant performance, and recommendations.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF06	Mission Qualification Training Review Assessments	3.2.2.2	Annually	COR
Description: A documented assessment of MQT products and events, reviewing for accuracy, completeness, and tactical relevance, including actionable recommendations for improvement.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF07	Aggressor Threat Replication Guide (in coordination with Intelligence)	3.2.2.2	Annually, with quarterly updates as required by new intelligence.	COR
Description: The complete and updated Aggressor Threat Replication Guide, developed in coordination with the intelligence shop to ensure threat realism and fidelity.				
[redacted]				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF08		3.2.2.2		COR

DRAFT

	Exercise and Mobile Teach Team Support Products and Instruction		1 month prior to exercise or as requested.	
Description: All products, briefing materials, and instructional content prepared for supporting exercises and mobile teach team events.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF09	OW Operator Support Reports (TDY days, Exercise Participation)	3.2.2.3	2 weeks following event.	COR
Description: A report summarizing operational support provided, detailing TDY days, specific exercises supported, and roles performed (e.g., OW operator).				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF10	Future OW Suite Cost-Benefit Analysis	3.2.2.3	Annually	COR
Description: A comprehensive report analyzing potential future OW suites, including research findings, technical capabilities, and a cost-benefit analysis for government consideration.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF11	Conference Plans	3.2.2.3	1 month prior to conference	COR
Description: A detailed plan for each conference, including objectives, agenda, attendee list, logistical details, and required briefing materials.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF12	Post-Conference Reports	3.2.2.3	2 weeks after conference	COR
Description: A summary report following each conference, detailing outcomes, key takeaways, action items, and a summary of any issues encountered and their resolution.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
BF13	Weekly Classified Intelligence Briefings on Adversary Space Activities	3.2.2.4	Weekly	COR
Description: The slide deck and any supporting materials for the weekly classified intelligence briefing, focusing on adversary space and space control activities.				

DRAFT

Identifier	Name	PWS #	Schedule	Distribution
BF14	Tailored Threat Assessments for Specific Training Audiences	3.2.2.4	As required, 15 days prior to the supported training event.	COR
Description: A threat assessment and briefing package specifically tailored to the training audience and their systems, based on the latest intelligence.				

Deliverable Table

Identifier	Name	PWS #	Schedule	Distribution
C001	Cyber Intelligence Analysis Reports	3.3.1	Weekly	COR & Ops Director and Ops Supe
Description: Threat based reports that are gathered using single or multiple sources across classifications to communicate to stakeholders an understanding of credible threats.				

Identifier	Name	PWS #	Schedule	Distribution
C002	Threat-Based Requirements Documents	3.3.1	Annual	COR & Ops Director and Ops Supe
Description: A database of all cyber threats and any systems/licenses needed to replicate these threats.				

Identifier	Name	PWS #	Schedule	Distribution
C003	Tailored Intelligence Products	3.3.1	As requested	COR & Ops Director and Ops Supe
Description: Documents and briefs that are tailored to a given exercise or operation.				

Identifier	Name	PWS #	Schedule	Distribution
C004	Mission Reports and Briefings	3.3.2	Post exercise completion	COR & Ops Director
Description: After action reports that include all Red Team actions on the network. List any problem areas that are encountered. Briefings should occur before and after exercises.				

DRAFT

FUTURE WORK

Identifier	Name	PWS #	Schedule	Distribution
CF01	Cyber Range and Aggressor Training Programs	3.3.3.1	Annual	COR & UTM

Description: Documentation that details the training program such as milestones, training efficiency & proficiency, training objectives.

Identifier	Name	PWS #	Schedule	Distribution
CF02	Training Materials	3.3.3.1	As Requested	COR & UTM

Description: Documents from training lessons that show training outcomes and training lessons.

Identifier	Name	PWS #	Schedule	Distribution
CF03	Trainee Performance Reports	3.3.3.1	As Requested	COR & UTM

Description: A roster of all trainees that includes dates of completion for training and when training is due. These reports should include any training certificates or diplomas.

Identifier	Name	PWS #	Schedule	Distribution
CF04	Adversarial Emulation Plans	3.3.3.2	As Requested	COR & Ops Director

Description: Detailed plans for adversarial emulation exercises and operations.

Identifier	Name	PWS #	Schedule	Distribution
CF05	Cyber Weapons and Tools Repository	3.3.3.2	Monthly	COR & Ops Director

Description: A repository of developed and procured cyber weapons, tools, exploits, and malware.

Identifier	Name	PWS #	Schedule	Distribution
CF06	Infrastructure Design Documents	3.3.3.3	Annual	COR & Range Director

Description: Network design to include all equipment and cabling/ports.

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
CF07	Uptime Reports	3.3.3.3	Monthly	COR & Range Director

Description: Reports that show how often the system goes down and how long it stays down. Uptime reports should show this as a percentage and as an hourly metric.

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
CF08	Security Vulnerability Reports	3.3.3.3	Monthly	COR & Range Director

Description: Reports that show how often the system goes down and how long it stays down. Uptime reports should show this as a percentage and as an hourly metric.

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
CF09	Vulnerability Assessment Reports	3.3.3.4	As requested	COR & Ops Director

Description: Report that details how the assessment was completed, any vulnerabilities with the risks to the range.

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
CF10	Meeting Minutes	3.3.3.5	As Requested	COR & Range Director

Description: Detailed minutes of stakeholder meetings detailing action items and decisions.

[redacted]

Identifier	Name	PWS #	Schedule	Distribution
CF11	Requirements Documents	3.3.3.5	As Requested	COR & Range Director

DRAFT

Description: Documents that overview the requirement from all stakeholders to include the provider, customer and the program office.

Identifier	Name	PWS #	Schedule	Distribution
CF12	Risk Assessment Reports	3.3.3.5	Annual	COR & Range Director

Description: Any risk to the program with details on what category it falls in (cost, schedule, performance).

Identifier	Name	PWS #	Schedule	Distribution
CF13	Red Team Operational Standards and Evaluation Criteria	3.3.3.6	Annual	COR & Ops director

Description: Standards that the trainees will be held to when they are evaluated. A list of all evaluation criteria with references to the standard.

Identifier	Name	PWS #	Schedule	Distribution
CF14	Personnel Evaluation Reports	3.3.3.6	As Requested	COR & UTM & Ops Director

Description: Records of how each member performed.

Identifier	Name	PWS #	Schedule	Distribution
CF15	Red Team Certification Database	3.3.3.6	Quarterly	COR & UTM & Ops Director

Description: Document of all certification and completion of Stan & Eval.

Identifier	Name	PWS #	Schedule	Distribution
CF16	Cyber Range Scenarios	3.3.5.4	Prior to all exercises	COR & Director Range Ops, Director, XP

DRAFT

Description: Exercise timelines, participants with roles and all desired learning objectives.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
CF17	Scenario Documentation	3.3.5.4	Prior to all exercises	COR & Ops Director
Description: Network diagrams that are needed to completed any desired learning objectives. This documentation should also include any agreements to partcipate in exercises.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
CF18	After-Action Reports	3.3.5.4	After all Exercises	COR & Ops Director
Description: Details on all positives and negatives from the Cyber Exercise. Details on who owns any fix actions and when they are due.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
CF19	Team Management Plans	3.3.3.8	As Requested	COR & Ops Director
Description: Details on how the team will operate and what training they will need to accomplish the mission.				
Identifier	**Name**	**PWS #**	**Schedule**	**Distribution**
CF20	Cyber Operation Execution Logs	3.3.3.9	As Requested	COR & Ops Director
Description: Any logs that are generated from participating in a mission or exercise.				

DRAFT

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	Space Aggressor EW Support	3.1	Performance is acceptable when: - Intelligence products are delivered on time and meet quality standards. - Mission planning documents are submitted accurately and prior to deadlines. - Adversary replication is realistic and effective. - All mission systems are maintained and available for exercises. - Training programs are executed effectively with certified instructors.
2	Space Aggressor OW Support	3.2	Performance is acceptable when: - A minimum of 40 hours of RPO and Space Battle Management instruction is delivered annually with high effectiveness. - At least 80% of trainees achieve OW operator certification. - All tasked exercises are supported with certified operators. - Future OW suite analysis is provided annually.
3	Space Cyber Range Support	3.3	Performance is acceptable when: - Cyber intelligence analysis reports are delivered within 48 hours and meet quality standards. - Red Team technical leadership is provided in accordance with all risk management protocols. - Realistic cyber range scenarios are developed and documented for all exercises. - All cyber operators and team chiefs adhere strictly to established Rules of Engagement (ROE).

DRAFT

Appendix A: Mission System Inventory Descriptions

Commented [MH14]: Copied from original PWS, requires review & update.

A.1. GPS Jammers

A.1.1. **General:** This GPS EA suite is a COTS suite of equipment built by the Space Aggressors as a standard GPS EA platform. This brute force noise EA system consists of either a dual high power amplifier (HPA) or a single HPA configuration, a standardized signal generation case, antenna(s), and necessary support equipment**.** Currently have 10 total systems.

A.1.1.1. **Amplifier Case.** The amplifier case(s) consist of either a dual amplifier or single amplifier configuration. Additionally, the amplifier case contains the required connectors, cables, couplers and splitters/combiners to route the signals. The target signals are combined, amplified, split, and routed for monitoring and transmission.

A.1.1.2. **Signal Generation Case.** The signal generation case contains two modems capable of producing signals at GPS frequencies and two line amplifiers to provide initial signal amplification.

After initial amplification, the signals are routed via cables to connectors to be routed to the amplifier case(s).

A.1.1.3. **Antennas.** A variety of linear polarized and circular polarized antennas are available to broadcast the hostile EA signals. Each antenna possesses unique attributes regarding gain, radiation pattern, power handling capability, and polarization to meet customers' requirements. The radhaz definition is the area surrounding an antenna in which a higher susceptibility to radiation exists. The area that we have defined is slightly different for each antenna that we use. However, we use the largest Radhaz area identified for every antenna that we use instead of using different sizes: 160 in front, 20 ft to each side

A.1.1.4. **Support Case.** The support case contains various ancillary equipment including a power generator radio frequency (RF) cable, spectrum analyzer, magnetic compass, inclinometer, and a tool kit.

A.2. **AN/USC-60A Flyaway Tri-band Satellite Terminal (FTSAT)**

A.2.1. **General:** The AN/USC-60A Flyaway Tri-Band Satellite Terminal (FTSAT) is a GOTS SATCOM system produced by L-3 Communications. This highly transportable system operates in the C, X or Ku bands. Space Aggressors use FTSAT as a "front-end" SATCOM EA terminal leveraging signal generation capabilities from systems such as the Badger. The system is comprised of the following: Antenna Group, Electronics Case, and HPA. Currently have 4 operational systems.

A.3. **Red Yak**

A.3.1. **General:** Red Yak. The Red Yak Version 2 MOD 1 UHF Military SATCOM (MILSATCOM) Interference System is a transportable jammer built by TMC Design Inc. and reconfigured by the Space Aggressors. Red Yak Version 1, as delivered by TMC Design, was a threat-representative system comprised of two truck-mounted shelters and two trailer-mounted antenna arrays. Version 2, reconfigured by the Space Aggressors, repackaged the terminal electronics of Version 1 into a three-case transportable system capable of worldwide use. Version 2 MOD 1 replaced the 500 watt amplifier with a 300 watt amplifier while retaining the ability to operate with the 500 watt amplifier prior to mission. The system is capable of transmitting a single signal of varying bandwidths and powers at a single frequency typically targeting one UHF channel at a time. Through the use of signal hopping, more than one UHF channel can be targeted simultaneously. The system is also capable of transmitting unencrypted analogue voice signals to replicate unauthorized UHF users**.** Currently have 2 total systems.

A.4. **Badger**

A.4.1. **General:** The Badger is a suite of COTS/GOTS equipment built by the Space Aggressors as a standard SATCOM EA signal generation platform to be used with available COTS/GOTS SATCOM terminals. This equipment can be utilized with the FTSAT, IMATE and GMT SATCOM systems. The Badger is equipped with one dual-channel signal generator and four SATCOM modems. The Badger may be used with a 70 MHz or an L-Band patch panel to allow it to interface with various SATCOM terminals. Each patch panel is capable of independently controlling four signal paths supporting EA operations. Currently have 4 total Badgers, which operate in L-Band.

A.5. **Integrated Multiple Antenna Terminal Electronics (IMATE)**

DRAFT

A.5.1. **General:** The IMATE is a single-hub suite of signal generation, amplifier control and antenna tracking hardware produced by L-3 Communications. The system is designed to interface and control a variety of satellite antennas operating in C, X, Ku, and Ka bands. Currently have 1 total system.

A.5.1.1. **HPA Controller.** IMATE is equipped with a controller, which allows the operator to locally or remotely manage the HPA from the front panel or a laptop computer.

A.5.1.2. **Antenna Control Unit (ACU) and Power Drive Unit (PDU).** The ACU interfaces with the PDU to enable satellite auto acquisition and auto track. Space Aggressors typically take advantage of the system's auto track function.

A.5.1.3. **Tri-Band Converters.** The tri-band block converters provide the required frequency up/down conversion (between L-band and RF) to enable signal transmission and reception in the C, X, and Ku bands.

A.5.1.4. **Ka Band Controller.** The Ka band controller provides remote configuration of the antenna Ka-band transceiver.

A.5.1.5. **Modem.** The IMATE comes equipped with a dedicated DMD-2050 SATCOM modem; but the system is capable of interfacing with external signal generation devices (such as the Badger).

A.5.1.6. **Data Collection Unit and Control Laptop.** The data collection unit (DCU) provides a common interface point between the laptop computer and other equipment making up the terminal.

A.6. **AN/TSC-179 Ground Multi-Band Terminal (GMT)**

A.6.1. **General:** The AN/TSC-179 Ground Multi-Band Terminal (GMT) is a dual-hub capable SATCOM terminal. It uses the same type of SATCOM modem, amplifier, amplifier control, and antenna tracking hardware as the IMATE system. As in the case of the IMATE, the GMT has the capability to operate in the C, X, Ku, and Ka bands. The primary difference between the GMT and the IMATE is the GMT is equipped with two hubs, 2.4 meter High Wind Antenna (HWA), Electronics Case and miscellaneous support test equipment. Currently have 2 total systems.

A.6.1.1. **High Wind Antenna (HWA)**. The HWA is a 2.4 meter, quad-band (C, X, Ku, and Ka) SATCOM antenna system. It is capable of automatic satellite acquisition and tracking and can be used with either IMATE or GMT terminals. The HWA is also known as the Small Aperture Antenna with certain production GMT terminals.

A.6.1.2. **Electronics Case.** The Electronics Case consists of two hubs. Each hub consists of three electronics cases.

- **Cases A and D.** Each case contains six modems. These modems may be used as alternate signal generation capacity in lieu of the Badger.
- **Cases B and E.** Each case contains a DCU, modem, HPA Controller, Trac 9000 timing distribution unit, and the local Fiber optic unit.
- **Cases C and F.** Each case contains an ACU, DCU, Tri-band Up/Down Converters, Test translator, Ka-Band Controller, Remote Fiber Optic Unit, and PDU.

A.7. **Test Measurement Diagnostic Equipment (TMDE)**

A.7.1. **General:** TMDE consists of COTS equipment used to generate, view, or manipulate the RF environment. Equipment includes spectrum analyzers, signal generators, oscilloscopes, vector signal analyzer, and a wattmeter. There is no in-house maintenance on this equipment. All maintenance is accomplished via PMEL as required. Currently have 146 items in USG inventory.

DRAFT

A.7.2. **TMDE is comprised of the following equipment:** Spectrum analyzers, signal generators, oscilloscopes, voltmeters, and various torque wrenches

A.8. **Generators**

A.8.1. **General:** 527 SAS maintains multiple power generators in various sizes located at Bldg. 815. Both gasoline and diesel generators are represented. Currently have 26 total generators, 23 3K and 3 11K generators.

A.9. **Cyber Assets/Programs/Equipment**

A.9.1. **Cobalt Strike**

A.9.1.1. **Description:** C2 application for adversary simulations and red team operations

A.9.2. **Parrot OS**

A.9.2.1. **Description**: Operating System for development testing

A.9.3. **Red Hat Enterprise Linux**

A.9.3.1. **Description**: Server operating system

A.9.4. **Windows Server 2016-22**

A.9.4.1. **Description**: Server Operating system

A.9.5. **Cisco Internetwork Operating System**

A.9.5.1. **Description**: Proprietary operating system that runs on Cisco Systems, routers, and switches

A.9.6. **VMWare**

A.9.6.1. **Description**: Software to run virtualized machine

A.9.7. **Python**

A.9.7.1. **Description**: Scripting language

A.9.8. **C/C++**

A.9.8.1. **Description**: Programming language

A.9.9. **Kali Linux**

A.9.9.1. **Description**: Operating system designed for penetration testing and digital forensics

A.9.10. **Aircrack-ng**

A.9.10.1. **Description**: Network software suite of tools for 802.11 wireless LANs

A.9.11. **Autopsy**

A.9.11.1. **Description**: software that makes it simpler to deploy programs and plugins

A.9.12. **Armitage**

A.9.12.1. **Description**: Graphical cyber-attack management tool that visualizes targets and recommends exploits.

DRAFT

A.9.13. **Burp suite**

A.9.13.1. **Description:** Web pentesting interception proxy

A.9.14. **BeEF**

A.9.14.1. **Description**: Pentesting tool targeting web browsers

A.9.15. **Cisco Global Exploiter**

A.9.15.1. **Description**: Pentesting tool exploiting Cisco switches and routers

A.9.16. **Ettercap**

A.9.16.1. **Description**: Man-in-the-middle attack suite

A.9.17. **Hashcat**

A.9.17.1. **Description:** Open-source network security tool for man-in-the-middle attacks on LAN

A.9.18. **John the Ripper**

A.9.18.1. **Description:** Password cracking tool

A.9.19. **Kismet**

A.9.19.1. **Description**: Passive network detector, packet sniffer, and IDS for 802.11 wireless LANs

A.9.20. **Lynis**

A.9.20.1. **Description**: Extensible security autdit tool for computer systems running Unix based OS's

A.9.21. **Maltego**

A.9.21.1. **Description**: Software used for intelligence and forensics

A.9.22. **Mimikatz**

A.9.22.1. **Description**: Open-source application that allows users to view and save authentication

A.9.23. **Metasploit framework**

A.9.23.1. **Description**: A tool for developing and executing exploit code against remote target machine credentials

A.9.24. **Nikto**

A.9.24.1. **Description**: Command-line vulnerability scanner that scans webservers for dangerous files/CGIs, outdated server software and other problems.

A.9.25. **Nmap**

A.9.25.1. **Description**: A network scanner used to discover hosts and services on a computer network

A.9.26. **OWASP ZAP**

A.9.26.1. **Description**: Open-source web application security scanner

A.9.27. **Sqlmap**

DRAFT

A.9.27.1. **Description**: SQL injection automation tool

A.9.28. **Wireshark**

A.9.28.1. **Description**: open-source packet analyzer

A.9.29. **Nessus**

A.9.29.1. **Description**: Proprietary vulnerability scanner

A.9.30. **Zenmap**

A.9.30.1. **Description:** GUI for NMAP

A.9.31. **Hydra**

A.9.31.1. **Description**: Parallelized network login cracker

A.9.32. **C/C++Reverse engineering toolkit**

A.9.32.1. **Description:** Programming language

A.9.33. **Foremost**

A.9.33.1. **Description**: Forensic data recovery program

A.9.34. **Volatility**

A.9.34.1. **Description**: Open-source memory forensics framework for incident response and malware analysis

A.9.35. **VulnHub**

A.9.35.1. **Description**: Offline virtual machines for creating private labs to practice hacking skills.

A.10. **Additional Equipment**

A.10.1. This list is not all inclusive as future capabilities and equipment may become part of the 527 SAS mission set. If new equipment and capabilities are added, contractors shall be expected to become SMEs in these areas. Training will be provided by the USG.

DRAFT

Attachment 1 – Government Furnished Property

DRAFT

Attachment 2 – Government Furnished Material

(HAF) OSD Memo - CMMC Implementati

DRAFT