Revised Performance Work Statement (PWS)
Wireless Network Deployment at SOCNORTH, Peterson Space Force Base

1. Purpose / Objective

The purpose of this effort is to design, develop, implement, test, and validate a Commercial Solutions for Classified (CSfC) Wireless Local Area Network (WLAN) Capabilities Package (CP) architecture to extend both the Secure Internet Protocol Router Network (SIPRNet) and the Non-classified Internet Protocol Router Network (NIPRNet) over a government-controlled network at the SOCNORTH Headquarters building located at Peterson Space Force Base, Colorado.

The contractor shall deliver a National Security Agency (NSA)-compliant wireless network solution nested within the USSOCOM Enterprise CSfC wireless architecture that meets the performance outcomes described in this PWS. This effort is a greenfield deployment for both CSfC and NIPR wireless capabilities.

The deployed WLAN shall serve as the primary source of work for the facility, requiring continuous, high-density, high-capacity sustainment to support current staff plus an additional 50-75 new personnel. The physical deployment footprint is strictly limited to the Western portion of the facility (approximately 60% of the ground floor, and 40% of the second floor). Contractors will not be working within the SCIF or the Top Secret East side.

The project shall be executed in phased increments governed by Contract Line-Item Numbers (CLINs) and associated Notices to Proceed (NTPs).

2. Scope of Work

The contractor shall provide all labor, supervision, management, materials, tools, transportation, equipment, cabling, testing equipment, penetrations, mounting hardware, and incidental services necessary to complete the tasks identified in this PWS. All work shall comply with applicable NSA CSfC Capability Packages, USSOCOM Enterprise Wireless requirements, applicable DoD Security Technical Implementation Guides (STIGs), NSA Common Criteria requirements, and industry best practices.

2.1 Phased Execution

CLIN 0001 – Study and Design (FFP)

Upon issuance of Notice to Proceed (NTP), the contractor shall:

- Conduct pre-onsite assessments (this is not mandatory).
- Conduct wireless site surveys utilizing AP-on-a-stick methodology where practical.
- Evaluate existing infrastructure and environmental readiness.

- Assess cybersecurity considerations applicable to the CSfC WLAN deployment.
- Develop and deliver High-Level Design (HLD) and Low-Level Design (LLD) documentation.
- Develop predictive and measured wireless heat maps.
- Develop a proposed milestone schedule, accounting for on-hand government furnished equipment (see appendix 1) that must be used for this project and a list of any additional equipment needed to execute this project along with procurement lead times.
- Submit final deliverables for government review and approval.
  Government acceptance of CLIN 0001 deliverables is required prior to issuance of NTP for CLIN 0002.

CLIN 0002 – Equipment Procurement and Installation (NTE FFP)
Following Government approval of the HLD/LLD and issuance of NTP, the contractor shall:

- Procure all required non-Government Furnished Equipment (GFE). Cost to government must be realistic, fair and reasonable.
- Provide a 1-year equipment and workmanship warranty for all procured and installed components.
- Perform all wall, floor, and ceiling penetrations required for cable routing and AP installation.
    - All new penetrations shall match existing with conduit sleeves, bushings, acoustical caulking, and 2hr fire rated caulking at all fire-rated walls.
- Provide all mounting hardware, lift equipment, and installation tools.
- Install, configure, integrate, and validate all WLAN components to include:
    - The installation of all required CAT6A shielded plenum-rated cabling.
    - Implementation and deployment of 802.1x Network Access Control (NAC) and RADIUS/NPS infrastructure.
    - Configuration of firewall policies to logically segment IoT, guest, user, and admin traffic.
- Implement dedicated Wireless Intrusion Detection System (WIDS) capability as required for NSA CSfC compliance when not satisfied by existing GFE.

- Implement high availability (HA) and redundancy using industry best practices consistent with the operational constraints of SIPRNet and NIPRNet services.
- Configure a dedicated, on-premises controller architecture for the CSfC WLAN environment.
- Implement RF containment strategies (e.g., directional antennas, power reduction, optimal AP placement) to ensure unclassified WLAN coverage does not unintentionally penetrate SCIF boundaries.
  The Government shall provide connectivity between IDFs and the MDF through existing fiber penetrations.

CLIN 0003 – Testing and Validation (NTE FFP)
The contractor shall perform testing and validation activities upon completion of installation activities and prior to Government acceptance. Testing activities shall include:

- End-to-end SIPRNet and NIPRNet connectivity validation to include but not limited to end user devices.
- RF coverage validation.
- Interference and redundancy validation.
- Configuration validation.
- STIG compliance validation.
- Security compliance checklist verification.
- Validation of CSfC WLAN implementation requirements.
- Proper documentation of the WLAN implementation.
- Post-installation wireless site survey and updated heat map generation.
  Testing shall not include penetration testing or red team assessment activities. Government personnel shall evaluate final operational standards for acceptance.

CLIN 0004 – Final Documentation (NSP)
The contractor shall provide final project documentation including:

- Updated wireless heat maps.
- As-built drawings and documentation.
- Final equipment inventories.
- Configuration backups and baseline configurations.

- Final testing and validation reports.
- Network integration diagrams.
- Site Wireless Security Operating Plan (SOP).
- Final project closeout package.
  All costs associated with CLIN 0004 shall be included within priced CLINs in accordance with contractor accounting practices.

2.2 Project Management

The contractor shall provide project management support throughout the Period of Performance, including:

- Conduct a kickoff project meeting within five (5) business days of award with SOCNORTH and USSOCOM.
- Maintaining an integrated project schedule.
- Providing weekly progress updates.
- Identifying schedule risks and mitigation strategies.
- Coordinating all Government access requirements and site activities.
- Serving as the primary technical and management liaison.
  For planning purposes, Government review periods for submitted deliverables shall be assumed to be five (5) business days.

2.3 Study and Design Requirements (CLIN 0001)

The contractor shall conduct assessments of:

- Existing infrastructure.
- Power and HVAC readiness.
- Existing pathways and penetrations.
- Cybersecurity posture relevant to the WLAN deployment.
- RF propagation characteristics that determine optimal Access Point (AP) placement, channel planning, and power settings.
- Coverage objectives and interference sources.
- Physical security considerations affecting SCIF and TEMPEST-certified environments.

- The contractor shall ensure WLAN implementation activities do not negatively impact existing SCIF, SAPF, or TEMPEST certifications. The cybersecurity assessment shall be limited to the scope of the CSfC WLAN deployment and integrated into the HLD and LLD deliverables with government oversight.
- The cybersecurity assessment shall be limited to the scope of the CSfC WLAN deployment and integrated into the HLD and LLD deliverables with government oversight.
- As the designated Trusted Integrator (TI) for the Commercial Solutions for Classified (CSfC) implementation, the Contractor shall perform a comprehensive technical assessment of the End User Device (EUD) baseline configuration to verify compliance with current CSfC Capability Package requirements, applicable NSA guidance, and all relevant Department of Defense (DoD) cybersecurity policies and security controls. This review will evaluate the operating system configuration, VPN architecture, security settings, authentication mechanisms, certificate management, endpoint protection requirements, and all CSfC-related configuration elements necessary to support accreditation and operational use.
- The assessment shall result in a documented, repeatable deployment baseline that can be consistently applied across all EUDs supporting the solution. Detailed installation, configuration, validation, and sustainment procedures shall be developed to ensure standardized deployment practices, reduce configuration drift, and support future scalability. The resulting documentation will serve as the authoritative implementation guide for all EUD provisioning activities and will support cybersecurity compliance, operational consistency, and lifecycle management requirements.
- The final EUD architecture shall align with the approved CSfC Campus WLAN implementation and ATO boundaries. The Windows EUD shall use the native Microsoft 802.1X supplicant for WLAN authentication (e.g., EAP-TLS with certificates), which provides network access to the protected wireless infrastructure and is not considered an Outer VPN client. The outer wireless access layer shall be provided by the approved Aruba infrastructure, including APs, switching, and Mobility Controller/Gateway operating within the CSfC security boundary. The EUD shall host a single VPN client to establish the Inner CSfC tunnel.
- The Inner encryption layer shall be implemented using Cisco Secure Client on the Windows EUD, terminating to the designated Cisco ASA as the Inner Encryption Component. The Contractor shall validate VPN configuration, cryptographic

settings, certificates, endpoint security controls, and supporting infrastructure in accordance with CSfC requirements, NSA guidance, DoD cybersecurity policy, and the approved system design, ensuring compliance with USSOCOM baseline architecture and SOCNORTH requirements.

2.4 Installation Standards

All installation and configuration activities shall comply with:

- NSA CSfC Capability Packages.
- USSOCOM Enterprise CSfC Wireless architecture requirements.
- Applicable NSA supplemental annexes.
- NSA Common Criteria requirements.
- DoD STIG requirements.
- Applicable federal cybersecurity standards.
- Applicable commercial cabling and installation standards.
- NIST SP 800-153 (Guidelines for Securing Wireless Local Area Networks). *Cloud-managed WLAN architecture shall not be utilized for this deployment*.

---

3. Deliverables and Schedule

The contractor shall submit a Proposed Milestone Schedule with an overall Period of Performance not to exceed 120 calendar days from contract award. Key deliverables include:

Deliverable	Due Date
Kickoff Meeting	Within 5 business days of award
High-Level Design (HLD)	15 business days after award
Low-Level Design (LLD)	30 business days after award
Installation Completion	Per approved milestone schedule
Testing and Validation Report	Within 5 business days of CLIN 0003 completion

As-Built Documentation	Within 15 calendar days of installation completion
Site Wireless Security Operating Plan (SOP)	Per approved milestone schedule

4. Period of Performance

The overall Period of Performance shall not exceed 120 calendar days from contract award. The contractor shall provide a milestone schedule accounting for equipment lead times and phased execution activities.

5. Government-Furnished Equipment and Information

The Government shall provide:

- Existing on-hand equipment is identified in Appendix 1.
- USSOCOM-approved Material Equipment Lists (MELs).
- USSOCOM baseline configurations.
- Gray Network links between USSOCOM and SOCNORTH, and configured encryption device between both sites.
- Existing fiber connectivity between IDFs and MDF.
- Government Points of Contact (POCs).
- Required site access to be coordinated to gain base access and building access.
- DD254 required at contract award.
- USSOCOM Enterprise Gray Site Validation Checklist documentation.

6. Performance Standards

The contractor shall meet the following performance objectives:

Requirement	Standard
Signal Coverage	95% of the designated coverage area (defined strictly as the West side of the ground floor and the non-Top Secret West side of the second floor) achieving -65 dBm RSSI or better

Signal Quality	Maintain minimum SNR of 25 dB
Security Compliance	Full compliance with NSA CSfC, STIG, and applicable federal standards
Schedule Performance	Completion in accordance with approved milestone schedule
WLAN Availability	HA and redundancy implemented per industry best practices

7. Security Requirements

The contractor shall comply with:

- The site visit will take place at Building 30 on Peterson Space Force Base, which is a restricted area and not open to the public. To reserve your attendance and meet installation access requirements, please provide the following information:
    - Full Name
    - Date of Birth
    - Driver's License number, city/state (must be current/active)
    - Submit the above information to luis.a.cibrian.civ@socom.mil , no later than 2 PM MT on 9 July 2026. Access cannot be guaranteed for late submissions.
- All vendors will request Visitors Access Request (VAR) from SOCNORTH prior to all visits, (SMO: CODE, SOCNORTHSO-CSMO-104) POC is Ms. Janice Coffman, Janice.coffman.ctr@socom.mil.
- For directions, see appendix 2, we recommend using the Peterson Space Force base visitors gate for base access.
- The executing contractor needs to be on the NSA CSfC approved trusted list to execute this contract for the government. Executing company is allowed to partner with an entity that:
    - Has a high-level technical knowledge and experience in executing these contracts.

    - And already partners with USSOCOM to provide technical expertise.
- Executing team will have at the minimum a secret clearance to install cables and access points.
- DD254 requirements, executing contractor must be cleared up to TS for the configuration portion of this project. See appendix 3.
- National Industrial Security Program Operating Manual (NISPOM) is a requirement.
- USSOCOM and SOCNORTH local security procedures.

Contractor personnel performing on-site work shall possess, at minimum, active Secret clearances at time of award. The Government will not sponsor new clearances for this effort. Subcontractors may be utilized provided the Prime Contractor remains compliant with FAR 52.219-14 and all applicable small business subcontracting limitations. A proposed subcontractor listed on the NSA CSfC Trusted Integrator List satisfies the Trusted Integrator requirement when proposed as part of the Prime Contractor team.

---

8. Assumptions and Constraints

- No cable runs exist. The contractor is responsible for installation of new cabling for proposed AP locations and cable runs back into the data center.
- Cable runs to APs shall not exceed 100 meters, exceptions to this rule will be made on a case-by-case basis.
- Ceiling heights are approximately 10–13 feet with drop ceiling construction.
- Contractors will provide all required lift and installation equipment.
- Wireless deployment activities shall not disrupt SOCNORTH missions or daily operations.
- Government-caused delays will be taken into consideration for extensions.
- Any delays related to KG link establishment shall be handled in accordance with FAR 52.212-4(f), Excusable Delays.
- Travel costs shall be incorporated into applicable CLIN pricing and shall not be proposed as separate ODCs.
- Site Wireless Security Operating Plan (SOP) will be required by HQ USSOCOM to ensure all site resources required to support initial operation and maintenance of the wireless solution are in place.

- Any aesthetic damage will be policed by the contractor to reinstate the premise to its original standards.
- The Government will be responsible for the Authority to Operate (ATO) process; however, the contractor must ensure the project is executed to USSOCOM and NSA standards to facilitate ATO approval.

9. Contract Line-Item Numbers (CLINs)

CLIN	Description	Contract Type
0001	Study, Site Survey, and Design	Firm-Fixed-Price (FFP)
0002	Equipment Procurement and Installation	Not-to-Exceed (NTE) FFP
0003	Testing and Validation	NTE FFP
0004	Final Documentation	Not Separately Priced

10. Points of Contact

Government POCs shall be provided upon contract award.