VTC/AV Lifecycle Support
Hill Air Force Base
Performance Work Statement (PWS)

1. SCOPE.

Successful award of this contract will provide sustainment of existing and future, traditional and Microsoft Teams-based, Video Teleconferencing (VTC) and Audio-Visual (AV) systems at Hill Air Force Base, the Utah Test and Training Range (UTTR), and Little Mountain Test Facility (LMTF). The Contractor shall provide:

- Technical solutions and design services for new and existing VTC or AV systems
- Procurement, installation of new VTC and AV systems
- User training for new VTC and AV systems
- Maintenance services

This contract requires the vendor to obtain necessary security clearances and coordinate with Hill Air Force Base personnel on matters involving security impact and cybersecurity compliance including DISA Security Technical Implementation Guides (STIG). The contractor shall provide resources, both technical and functional, required for managing contract performance.

1.1 **VTC/AV Maintenance Activity Report (MAR):** Contractor shall provide the 75 ABW SC COR, a MAR detailing support requests, response times, and resolution. The MAR will include the status of all active tickets during the previous month, including open and closed tickets. The contractor shall include effort to meet STIG compliance, if any. The contractor shall deliver the report to the COR, via email, by the 5th business day of each month. (CDRLA001)

1.2 **Staffing Roster**: Within 10 business days of contract award, Contractor shall provide a list of all personnel who could be called upon to support this contract. Additions to and removal of personnel will be identified to the 75ABW/SC Security Manager within five (5) business days of the change in accordance with (IAW) Section 3.9 of this contract. (CDRLA002)

Contractor shall ensure implementation services are performed by industry certified technicians including InfoComm CTS-D and CTS-I certified team members as well as by technicians holding a minimum of AVIXA CTS certifications. Contractor will provide proof of Certifications, upon request by the 75 ABW/SC COR.

1.3 **User Documentation and Training:** Contractor will provide operational training for newly installed systems and ensure customer has copies of all user manuals (digital format preferred) as part of final acceptance inspection. Contractor will report on user training activities in the VTC/AV Maintenance Activity Report. (CDRLA003)

2. REQUIREMENTS.

2.1 **Technical Solutions and Design Services.**

Contractor shall provide expertise to implement or upgrade VTC and/or AV systems, all requirements/projects must be approved by 75ABW/SC. Contractor shall attend meetings and site walks with the customer and 75 ABW/SC personnel to fully understand requirements.

Proposed solutions will include:

- Complete list of components
- Costs for equipment, delivery, engineering and installation, and monthly maintenance
- proposed schedules
- block diagram to indicate all connection points of the system

When possible, the contractor shall propose a solution to support Teams, or the currently approved web-based conferencing solution, over traditional VTC.

2.1.1 All proposed VTC and A/V technical solutions will comply with the following security guidance.

DISA STIGs and SRGs (Technical Implementation)
Enterprise Voice, Video, and Messaging Endpoint SRG
Unified Endpoint Management Server & Unified Endpoint Management Agent SRGs
Network Infrastructure Policy STIG
Traditional Security Checklist
Any Vendor-Specific STIGs

Department of the Air Force (DAF) Guidance	
DAFMAN 17-1301	Computer Security
DAFMAN 17-1302	Communications Security (COMSEC)
AFI 17-130	Cybersecurity Program Management
DAFMAN 17-1203	Information Technology Asset Management (ITAM) and Accountability
DAF Memo	Security Guidance for the use of Collaboration Peripherals and Capabilities in Secure Spaces
AFSSI 7700	EMSEC / TEMPEST
AFSSI 7011	Protected Distribution Systems (PDS)

DoD / DoW Policy Directives	
DoDI 8100.04	DoD Unified Capabilities
DoDI 8500.01	Cybersecurity
DoDI 8510.01	RMF
DoDM 5200.01, Vol 3	DoD Information Security Program

Federal, NIST, and CNSS Standards	
CNSSI 5000	Guidelines for Voice over Internet Protocol
CNSSI 7003	Protected Distribution Systems (PDS)
NIST SP 800-53	Security and Privacy Controls

NIST SP 800-115	Technical Guide to Information Security Testing and Assessment
Methods and Procedures Technical Order (MPTO) 00-33B-5006	Endpoint Security for Information Systems
FIPS 140-2 / FIPS 140-3	Cryptographic module standards

2.2 **Purchasing and Installation.**
Upon acceptance of proposed solution, Contractor shall provide all components necessary to implement a complete, fully functional system to meet requirements detailed in the accepted technical solution. Contractor shall provide status of hardware ordering, processing, shipping, tracking and project management.

Contractor shall manage industry-standard warranty issues for all new components installed. Contractor shall provide one-year labor warranty.

Technicians shall follow industry standards to ensure easy replacement of components due to failure.

Contractor shall ensure a clean and professional appearance of the space after final system installation is complete.

Contractor shall complete installation of additional LAN drops, as required to support a new or existing system. All work shall be accomplished in compliance with UFC 3-580-01 and the Hill Air Force Base Comm Standard (formerly Tab K) and in coordination with 75ABW/SC.

After system installation is complete, and in the presence of the purchasing organization and 75 ABW/SC personnel, Contractor shall perform a complete system test to ensure all features and functionality meet requirements. When the solution is proven to satisfy all requirements, the purchasing organization will formally accept the system.

2.2.3 **System Documentation.** The contractor shall provide system documentation including but not limited to schematics, wiring diagrams, and interconnection diagrams, to 75 ABW/SC, upon installation, when configuration changes are required, or upon request.

Contractor shall provide user training and user manual upon installation, testing, and acceptance of new systems.

2.2.4 **Packaging, Packing, and Shipping.** The contractor shall be responsible for all costs associated with shipment of equipment for repair and/or replacement, including loaner or spare equipment.

2.3 Maintenance Services.
Contractor shall provide on-going maintenance including but not limited to testing, repair, replacement, technical support, and support services for installation, training, and hardware and/or software upgrades.

2.3.1 **Security Technical Implementation Guides (STIG) Compliance.** The contractor shall ensure compliance with STIGs and OEM specifications through quarterly inspections. Results of these inspections shall be included in the Monthly Report (CDRLA001). 75 ABW/SC may request a compiled list of all VTC/AV systems inspection status.

2.3.2 **Current Systems.** Hill Air Force Base currently hosts active High or Mixed Use VTC systems as well as Microsoft Teams systems. Any organization, in coordination with the 75ABW/SC COR, may exercise the IDIQ option and provide payment for services or systems. The systems are categorized as follows:

Complexity Level	Description
TIER 3 Low (Maintenance and support services)	• Provides maintenance and support services of MS Teams only solutions
TIER 2 Low (Unclassified VTC and AV Systems)	• Provides unclassified video teleconferencing • Includes minimum amount of equipment supporting video teleconferencing capability • Low complexity teleconference environment
TIER 1 High or Mixed Use (Classified VTC or AV Systems)	• Provides secure video teleconferencing capability • Includes higher level of equipment and devices enabling the video teleconference capability • Provides the ability to select between secure and unsecure channels utilizing the same CODEC and video teleconferencing equipment providing dual capability • A complex teleconferencing environment

2.3.3 **Monitoring:** Contractor shall monitor existing systems for end of life (EOL) notifications and STIG compliance. See paragraph 2.3.1 for reporting requirements.

2.3.3.1 The contractor shall monitor and evaluate VTC and AV systems to ensure compliance with the appropriate Department of Defense (DOD)-approved architectures, programs, standards and guidelines, such as Defense Information Systems Agency's (DISA) Video Teleconferencing Security Technical Implementation Guide (STIG), web link: https://www.cyber.mil/stigs

2.3.3.2 When components reach EOL or are non-compliant with STIG requirements, the contractor shall notify the 75 ABW/SC COR of the problem, within three (3) days, and provide written recommendations, to address the problem and associated security risks. The contractor's primary responsibility under this section is fulfilled upon providing written notification and recommendations to the COR. The Government assumes the risk for operational status of non-compliant systems pending a funding decision.

2.3.4 **Staffing Requirements.** The Contractor shall have sufficient technicians available to respond to repair orders IAW this PWS, regardless of the number of reported repair orders, locations of the facilities, or systems requiring repair service.

75 ABW/SC will provide a workspace, desktop computer, and phone, available to technician(s) when on base.

2.3.4.1 Contractor personnel must be able to communicate effectively to ensure understanding of problem resolutions with Customers and 75 ABW/SC personnel.

Contractor personnel shall be qualified and maintain certifications as listed throughout this PWS and required by DoD 8570.01, at time of contract award and throughout the duration of the contract. See DoD 8570.01-M, Chapter 2, Figure C2.F1 for the Overview of Basic Information Assurance (IA) Workforce Structure.

2.3.5 **Request Tracking and Coordination**. The COR or 75ABW/SC-designated representative will coordinate incoming requests for VTC and/or AV maintenance support and services, assigning the ticket to a Project Manager who will coordinate with the contractor and system owner.

The Contractor shall respond to requests for maintenance within the timeframes specified below.

- Emergency (Critical) 4 Business Hours
- Routine (Medium) 2 Business Days
- Minor (Low) 3 Business Days

2.3.6 **Corrective Maintenance**. 75 ABW/SC COR has final determination in categorization of repair assigned to each problem/repair order, and 75 ABW/SC COR may elevate any corrective repair to a higher level. The contractor shall evaluate problem reports and complete corrective maintenance IAW the category of repair (Minor, Routine, or Emergency) referenced below. If repair is not possible, the contractor will provide written recommendation to resolve the failure, within three (3) business days.

The contractor shall maintain record of resolution actions for inclusion in the MAR.

2.3.6.1 **Minor Repairs**. Minor issues include color distortion on monitor, on/off light malfunctions on microphone, or other situations that do not prevent performance of the VTC or AV system. The contractor shall resolve reports of minor issues within seven (7) business days unless 75 ABW/SC COR approves additional time.

2.3.6.2 **Routine Repairs**. Scenarios such as a single malfunctioning camera or near/far end monitor malfunction that impede the VTC or AV system from continually performing video teleconferencing or AV communication functions are routine and should be resolved within five (5) business days unless 75 ABW/SC COR approves additional time.

2.3.6.3 **Emergency Repairs.** Emergency issues include codec malfunction or room controller outages which prevent the VTC and AV system performance from satisfying

real world operational missions, Life/Safety/Health and Senior Leader requirements. The contractor shall provide onsite maintenance within four (4) hours of notification for emergency repairs and resolve orders for emergency repair service within one (1) business day unless 75 ABW/SCOI approves additional time.

2.3.7 **VTC and AV Hardware Replacement.** The contractor shall only replace hardware, necessary to restore VTC and AV operations to normal service levels, when repair of the component would cost more than replacement. The contractor shall provide written recommendation for replacement items and costs to 75 ABW/SC COR. 75 ABW/SC COR or designee will evaluate the recommendation, obtain funding from system owner, and execute the purchase with the Contractor. Upon receipt of components, Contractor will perform installation to restore system functionality

2.3.7.1 Upon failure of component(s) outside of manufacturer warranty coverage, the system owner will bear responsibility for the cost to purchase the component(s) and labor to complete installation and restore the system to expected functionality.

3.0 GENERAL INFORMATION.

3.1 Common Access Card (CAC)

Contractor shall complete the organization's In-Processing Checklist (if applicable). Contractor shall present document(s) that establish identity; acceptable document(s) include: valid driver's license with photograph, name, date of birth, gender, height, eye color and address; ID card issued by federal, state, or local Government agencies with photograph, name, date of birth, gender, height, eye color and address; U.S. military card; military dependent ID card. A Common Access Card (CAC) is required for all on-site Contractor personnel. The Government shall provide appropriate identification cards which shall be issued, displayed and surrendered as directed in HAFBI 31-101, Installation Security Program. The Contractor Program Manager shall ensure that all employees have the proper identification credentials prior to entering Hill AFB. CACs are used for identification and network access. CACs are not to be worn off base, photographed, or reproduced in any manner. The Contractor shall return all credentials to the organization's security managers or Government Contract Office Representative (COR) and out-process via the organization's Out-Processing Checklist, if applicable, upon termination from the contract or contract completion.

3.2 Restricted Area Badges and Access to Controlled Areas

The Contract Manager or alternate shall complete an AF Form 2586, Unescorted Entry Authorization Certificate, for each employee requiring unescorted entry into controlled areas IAW HAFBI 31-101. The request shall be coordinated through the 75 ABW/SC Security Manager. If approved, employee shall present the AF 2586 to 75 SFS Pass and Identification, building 408 for processing. Employee will receive AF Form 1199C (commonly known as line badge). Employee must return AF 2586 to the organization’s security manager. The form will be needed when changes to the card are requested. When the badge is no longer needed, employee shall pick up the AF 2586 from the organization's security manager and take to 75 SFS to turn in. Employee shall return the AF 2586 to the organization's security managers. The controlled area badges shall be surrendered as required in HAFBI 31-101.

3.3 Access to the Network

- Non-Privileged: We will grant non-privileged access IAW AFMAN 33-282.
- Limited Privileged: We will grant limited privilege access in IAW AFMAN 33-282.

3.4 Computer Connectivity

The Government will provide connectivity to the base systems for Government official business for the number of connections required to perform services for this contract. The Contractor shall confine PC/Laptop system configurations to the current Government Standard Desktop Configuration (SDC). Any requests for variations will be submitted to the COR and approved by the Government prior to implementation. Contractor owned equipment shall not be permitted connectivity to the base network

3.5 Virtual Private Network (VPN)

The Contractor shall not use Contractor owned equipment for VPN access. Only Government owned equipment may be used for VPN access. The Contractor shall submit requests for VPN access in writing to the COR. The request shall include justification and specific personnel that shall utilize access; if approved, the Government will provide sufficient equipment for the Contractor to utilize. The equipment will remain Government property and reside on the Contractor's ADPE account for the duration of the approved period.

3.6 Foreign Object Damage (FOD) and Drop Object Prevention (DOP)

Contractor personnel who, in the performance of their assigned duties on this contract, work in, on, around, or travel through areas near aircraft, munitions, aerospace ground equipment (AGE), engines, or components shall comply with FOD prevention requirements prescribed in AFI 21-102.

3.7 General Contract Information

The Contractor shall be responsible for work requirements and work in progress no later than the end of the transition period as defined in Section 3.23. Although it is the responsibility of the Contractor to recruit, retain, and retrain, its employees, the Contractor shall ensure that all employees performing under this contract read, write, speak, and understand English at a technical level and proficiency adequate to the nature of the tasks assigned.

3.8 Contractor Employees

The Contractor shall provide the initial list of personnel who will support this contract no later than 10 working days after award of contract, and no later than 5 working days after hire of new employee (CDRLA002). Contractor shall provide updated lists as personnel changes occur within 5 business days of the change. The Government shall not be obliged to accept performance by any Contractor employee the contracting officer has identified to the Contractor as a threat to the health, safety, or general well-being of any other person on the installation. The Contracting Officer reserves the right to direct the Contractor to remove any employee from the worksite for reasons of misconduct or for failure to comply with security regulations. Moreover,

the Government shall not be obligated to accept performance from any Contractor employee the contracting officer has identified to the Contractor as a threat to good order and discipline, to Government property, or to any Government operation or mission. The Contractor shall ensure personnel obtain favorable local files checks or favorable National Agency Checks, reference Section 3.3, prior to applying for network access.

3.8.1 The Contractor shall not employ any person who is an employee of the United States Government if the employment of that person would create a conflict of interest, nor shall the Contractor employ any person who is an employee of the Department of the Air Force, either military or civilian, unless such person seeks and receives approval according to the DoD 5500.7-R Joint Ethics Regulations (JER). In addition, the Contractor shall not employ any person who is an employee of the Department of the Air Force if such employment would be contrary to the policies contained in AFI 64-106, Air Force Industrial Labor Relations Activities. The Contractor is cautioned that off-duty active military personnel hired under this contract may be subject to permanent change of station, change in duty hours or deployment. Military Reservists and National Guard members may be subject to recall to active duty. The abrupt absence of these personnel could adversely affect the Contractor's ability to perform. Their absence at any time shall not constitute an excuse for nonperformance under this contract. The Contractor shall not perform this contract in a manner that creates a conflict of interest or the appearance of a conflict of interest vis-à-vis Government employees, e.g., by requesting Government (COR) to survey Government contracts, subcontracts during their off-duty hours.

3.8.2 The Contractor shall ensure that its employees conduct themselves in a professional and courteous manner and that they present a neat and professional image appropriate to their duties to include wearing suitable attire and protective clothing as appropriate. The selection, assignment, reassignment, transfer, supervision, management, and control of Contractor employees shall be the responsibility and prerogative of the Contractor; however, the Contractor shall comply with the requirements set forth in this PWS and Hill AFB regulations concerning conduct of employees as referenced herein. Contractor personnel shall comply with directives pertaining to operation of privately owned vehicles on Hill AFB per AFMAN 31-116, Motor Vehicle Traffic Supervision. The Contractor shall employ and maintain a technically trained and experienced work force.

3.9 Hours of Operation

Contractor personnel shall perform the services required under this contract between the hours of 0800 (8:00 am) through 1600 (4:00 pm), totaling not more than 80 hours of service within a two-week period, unless otherwise notified by the Government.

The Contractor shall optimize personnel staffing and manning to match the PWS requirements and performance criteria between these hours. The Contractor shall perform the services required under this contract during office hours normally followed by the customers.

The hours of operation are subject to change and can be different for each area of operation. The Government will provide specific work hours for the Contractor upon request.

3.9.1 The Contractor is not required to provide service on the Federally approved holidays including the following:

- New Year's Day
- Martin Luther King Day
- Presidents Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veterans Days
- Thanksgiving Day
- Christmas Day

If the holiday falls on Saturday, we will observe the holiday on the previous Friday. If the holiday falls on a Sunday, we will observe the holiday on the following Monday. The Contractor may be required to observe all energy days and/or other down days as directed by OO-ALC Center Commander and/or AFMC at no cost to the Government.

3.9.2 On occasion, services may be required to support an activation or exercise of contingency plans outside the normal duty hours described above. The Contractor's responsibilities for after-hours support will be defined in the workload data. This is an unplanned event that would require staff that would need to be able to communicate and perform services for Base infrastructure.

3.9.3 The Contractor shall plan for and respond to mission requirements in the event of mobilization, terrorism, natural disaster, or labor disputes. Upon notification by the CO of the requirement to support these operations the Contractor shall provide documentation for all hours worked.

3.9.4 Within 60 minutes of notification by the CO, the Contractor shall provide services to support national commitments up to and including a declared war that would generate increased mission requirements. These services shall be provided 24 hours a day, seven (7) days a week, as required.

3.9.5 The Contractor shall provide the CO a completed plan for providing maximum support of contingencies. Additionally, the Contractor shall be aware of provisions contained in DODI 3020.37, Section 6.6 concerning Government contingency plans. The Contractor shall comply with DODI 3020.37, Sections 6.9 and 6.10.

3.10 Security Requirements

The highest classification for this requirement is SECRET. The Contractor shall ensure personnel have obtained a favorable local files check or favorable National Agency Check ref: Section 3.3, prior to applying for network access. (The 75 SFS Local Files Check is insufficient for this requirement.) The Contractor shall comply with all security and threat related

requirements as specified in DOD 5220.22M, National Industrial security Program Operating Manual (NISPOM); AFI 16-1404, *Air Force Information Security Program*; AFI 16-1406, *Air Force Industrial Security Program*; Hill Air Force Base Installation Anti-Terrorism Plan 10-245; AFI 36-3026 V1_IP; *Identification Cards for Members of the Uniformed Services, their Eligible Family Members and Other Eligible Personnel*, HAFBI 31-101 Installation Security Instruction, HAFB Plan 31-101, Installation Security Plan and subsequent instructions. The Contractor shall comply with Air Force policy to identify, mark, protect, and destroy classified information and material consistent with national policy IAW AFI 16-1404.

3.10.1 This contract has classified requirements described in form DD254 and the contractor shall adhere to all addendums and provisions of the DD254. Contractor shall adhere to all OPSEC requirements contained in the DD254 and this performance work statement.

3.11 Security Clearance Investigations

All Contractor personnel must meet the terms of this PWS and must be United States citizens. Applicable directives include DOD 5200.2-R and AFI 31-501. Any costs associated with obtaining a security clearance shall be the responsibility of the Contractor.

3.11.1 Personnel assigned shall have access to information that could cause serious damage; therefore, Contractor personnel assigned to those areas shall obtain or possess a SECRET clearance. IAW AFI 16-1406, paragraph 2.4, Industrial Security Program Management, when Contractors require unescorted entry to restricted areas, access to sensitive unclassified information, access to Government information systems and/or sensitive equipment, not involving access to classified information, the Contractor's personnel security questionnaire is processed by the sponsoring Air Force activity per DOD 5200.2-R and AFI 31-501, Personnel Security Program Management.

3.11.2 At contract start date and duration of contract, all Contractor personnel requiring elevated rights accounts to perform assigned duties shall possess a SECRET clearance or interim SECRET clearance.

3.11.3 When services are required in a Classified Processing Area (CPA), the contractor shall be escorted by a customer representative with sufficient clearance of open/close the CPA.

3.12 Non-Disclosure

The Contractor shall not divulge any information about files, data, processing activities or functions, user ID’s, passwords, or other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor personnel shall abide by all agency rules, procedures, and standards of conduct. The Contractor personnel shall comply with the Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Contractor Employees. The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201. The Contractor shall insert this clause in all subcontracts when the sub-Contractor is required to have physical access

to a federally controlled facility or access to a Federal information system. The Non-Disclosure Statement shall be due within 10 days of request by the Government. The Government is not obliged to accept performance from the Contractor or any of its employees who decline to sign or otherwise fail to execute a non-disclosure agreement.

3.13 Quality Control

3.13.1 Quality Control Program

The Contractor shall establish a complete quality control program to ensure the requirements of this contract are provided as specified.

3.13.2 Quality Assurance

The Government will periodically evaluate the Contractor's performance IAW the Service Summary Table and Government Quality Assurance Surveillance Plan (QASP) by appointing a COR to monitor performance to ensure services are received. The Government Contract Officer Representative (COR) will evaluate the Contractor's performance through intermittent on-site inspections of the Contractor's quality control program (para. 1.3) and receipt of complaints from base personnel. The Government may inspect each task as completed or increase the number of quality control inspections if deemed appropriate because of repeated failures discovered during quality control inspections or because of repeated customer complaints. Likewise, the Government may decrease the number of quality control inspections if merited by performance. The Government will also investigate complaints received from various customers located on the installation. The Contractor shall be responsible for initially validating customer complaints. However, the Government representative shall make final determination of the validity of customer complaint(s) in cases of disagreement with customer(s).

3.13.3 Contract Officer Representative (COR)

The COR is the authorized Government representative(s) who will perform assessments of the Contractor's performance. The COR or alternate(s) will inform the Contractor when discrepancies occur via a Contractor Performance Assessment Report (CPAR) and will request corrective action. The COR or alternate(s) will make a notation of the discrepancy on their assessment checklist with the date and time the discrepancy was noted and will request the Contractor to initial the entry on the checklist. Any matter concerning the scope, prices, terms or conditions of this contract shall be referred to the Contracting Officer and not to the COR. The services performed by the Contractor, during the period of this contract, are subject to review by the Contracting Officer or authorized representative(s).

3.14 Freedom of Information Act (FOIA)/Privacy Act

All official Government records affected by this contract are subject to the provisions of the FOIA and Privacy Act. Any request received by the Contractor for access/release of information from these records to the public (including Government/Contractor employees acting as private citizens), whether oral or in writing, shall be immediately brought to the attention of the Contracting Officer. All FOIA requests must be submitted through the Base FOIA Manager to ensure proper processing and compliance.

3.15 Operations Security (OPSEC)

All Contractors, subcontractors, their employees, associates, and consultants who have access to critical information must comply with Air Force Instruction (AFI) 10-701, Operations Security (OPSEC), and applicable local guidance. OPSEC is a systematic means of identifying and protecting information which an adversary could use against the interests of the US. The critical information list (CIL) identifies sensitive information which requires protection. Counter-measures (CM), sometimes called OPSEC measures (OM), are control standards with which all personnel must comply to protect critical information, within AFI 10-701.

3.15.1 Responsibilities: Prior to bid, the Contractor is advised to assess program requirements via AFI 10-701. Due to sensitivity, the following cannot be provided prior to contract award: The sponsor must provide or approve OPSEC training curriculum for use by the Contractor. Training must include awareness topics, CIL, CM/OM, threat/vulnerability, awareness of family/friends, and disciplinary action for non-compliance. The following will be provided (if not included in provided training materials): CIL, CM/OM, adversarial collection threat, OPSEC guidance (AFI 10-701 and applicable local guidance) specifically as it applies to the sponsor's organization, mission, and the contract.

3.15.2 The Contractor must identify personnel who will have access to critical information and ensure they have completed required OPSEC training IAW AFI 10-701, Chapter 5, prior to allowing access to critical information. The Contractor shall provide or ensure personnel attend Government supplied training as approved or provided by the sponsor. The Contractor may create or adapt OPSEC training in lieu of sponsor provided training, provided the new training is reviewed and approved by the sponsor. The Contractor may request approval from the sponsor to streamline refresher training by removing awareness topics IAW AFI 10-701, paragraphs 5.2.1 and 5.2.2 (only personnel for which a record exists indicating they have been trained on OPSEC awareness at some previous point in their career), organizational and contract specific training must be continued IAW AFI 10-701, paragraphs 5.2.3 and 5.2.4. The Contractor must track OPSEC training statistics including total number of personnel with access to critical information, a list of their names, date of OPSEC training completion, and when annual refresher training is due. Training must be provided before personnel are allowed access to critical information. The Contractor must ensure all personnel comply with OPSEC standards and practices as trained. Training may require modifications based on updates to critical information, CM/OM, intelligence threat, or other fundamental changes to the OPSEC program. Prior to seeking approval through Hill AFB Public Affairs, any information to be released outside of official U.S. Government channels, via any media, must be coordinated through an OPSEC review by (Gov. Organization's OPSEC program manager/coordinator).

3.16 Key Control

The Contractor shall establish and implement methods of ensuring all facility keys/key cards issued to the Contractor by the Government are not lost, misplaced and are not used by unauthorized persons. NOTE: All references to keys also include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures

covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel that no longer require access to locked areas.

3.16.1 The Contractor shall immediately report the occurrences of a loss of a key to the COR.

3.16.2 In case of loss or duplication of keys, other than master keys, the Contractor shall, upon written direction of the contracting officer, re-key or replace the affected lock or locks. The Government, at its option, may replace the affected lock(s) or perform re-keying, deduct the cost of re-keying or lock replacement from the monthly payment due the Contractor if Contractor negligence is found. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

3.16.3 The Contractor shall prohibit the use of keys issued by the Government by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor's employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the CO.

3.17 Lock Combination

The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations.

3.18 Records

The Contractor shall be responsible for creating, maintaining, and disposing of only those Government required records that are specifically cited in this PWS or required by the provisions of a mandatory directive listed in Addendum IV, Applicable Publications and Forms.

3.18.1 All official records (regardless of media) as defined in 44 U.S.C. Part 3301 / AFI 33-364 and AFMAN 33-363 are the property of the U.S. Government and shall remain so upon termination or completion of this contract.

3.19 Training

Contractor is responsible for maintaining the applicability and currency of all licenses, certifications and qualifications associated with the applicable labor categories. All training records for personnel must be maintained by the Contractor and be made available for Government inspection upon request. The Government's intent with this requirement is to ensure that personnel providing service are continually attaining required training, and currently licensed and certified for their assigned tasks. These training requirements are continuously subject to changes as industry and policy demands.

3.19.1 Government-Provided Training

The Government may provide training as required and as approved by the COR or 75 ABW/SC Unit Training Manager including but not limited to those listed below. All training must be approved by the Functional Director or COR prior to attendance. Most, but not all, of the training is provided via CBT.

Course Nbr	Title
C11681	Air Force Risk Management Fundamentals Course 2020
CHQSCI0000100DL	Level 1 STINFO Training (CBT)
MHPADM0003146CB	75 ABW/SC Operational Risk Management
MHPADM0265600DL	75 ABW/SC Annual Operation Security (OPSEC) Training
MHPADM0312800DL	75 ABW/SC Unit Emergency Management Training
MHPADM9800100DL	Identifying and Safeguarding Personally Identifiable Information (PII)
MHPADM9800500BR	Annual Drug-Free Federal Workplace Training
MHPCOM9800500VS	Using Mobile Devices in a DoD Environment
MHPSAF9801502BR	75 ABW/SC Annual Safety Awareness
MHPSAF9801800BR	GHS Chemical Labeling and SDS Retrieval Training - One-Time
MHPSEC9802900BR	Annual Training for Cleared Personnel
MHPSEC9803000BR	75SC NATO Security Awareness Brief
MLMW0279	DoD Combating Trafficking in Persons (CTIP) General Awareness Course
MLMW0432	DAF-Operations Security Awareness Training
MLMW2260	TFAT-Annual Cyber Awareness Challenge
MLMW2289	DoD Mandatory Controlled Unclassified Information Training
MLMW2655	AFQTPXXXXX-222RA, Records Management - User Training

3.20 Continuing Training

The Contractor retains full responsibility for ensuring its employees are adequately and appropriately trained to carry out their duties as assigned by the Contractor under this contract. Continuous e-Learning is available via the Air Force Portal. Most of these courses require Contractor funding for contract employees.

3.21 Emergency Situations

The CO/COR shall notify the Contractor when emergency situations exist (e.g., natural disasters, weather-related situations, base closures), which may cause changes to installation operations tempo.

3.22 Environmental Controls

3.22.1 Compliance with Laws and Regulations

The Contractor shall be knowledgeable of and comply with all applicable Interstate, Federal, State, and Local laws, regulations, and requirements regarding environmental protection. In the event environmental laws/regulations change during the term of this contract, the Contractor is required to comply as such laws come into effect

3.22.2 Notification of Environmental Spills

If the Contractor spills or releases any substance contained in 40 CFR 302 into the environment, the Contractor or its agent shall immediately report the incident to Hill AFB Fire Dept. at 777-

1911. The liability and costs associated with the spill or release of such substance(s), to include fines imposed on Hill AFB, damages and clean up, rests solely with the Contractor and its agent.

3.22.3 Material Storage and Use

The Contractor shall follow manufacturer's guidelines and professional recommendations for control of humidity, temperature, cleanliness, and materials handling.

3.23 Orientation/Transition Period

Estimated to be 30 days. The Contractor shall ensure a seamless transition to the maximum extent practicable. The Contractor's orientation plan shall demonstrate how personnel, materials and equipment will be utilized through the orientation period and a method to ensure performance and to include phase-in timelines. The plan shall also include the number and position titles of personnel to be on site for the orientation period. The Contractor shall begin the orientation and provide a written transition plan. The purpose of the orientation plan is to demonstrate how the Contractor shall meet the following:

3.23.1 Observe work accomplished by current employees and become thoroughly familiar with work requirements.

3.23.2 Complete personnel requirements (work force), including the hiring of personnel to assure satisfactory performance. Soliciting Government or Contractor personnel for employment during their duty hours is prohibited unless interview arrangements are made through the CO and personnel offices at this installation.

3.23.3 Complete Security requirements as identified in the PWS Paragraph 3.10.

3.23.4 Complete documentation and requests during the orientation period for all applicable security clearances or NACs, NACIs (if required by HSPD-12), or acceptable local files checks within two weeks of contract award.

3.23.5 Complete the development of necessary work plans and procedures based on PWS requirements.

3.23.6 The Contractor shall be allowed access to the facilities to familiarize supervisors, key personnel and staff with equipment, reporting, work scheduling and procedures. However, such access shall not interfere with the production efforts of current workforce. To preclude such interference, arrangements for access to the Government facilities shall be made with the COR.

3.23.7 If there is a change in Contractor or upon contract completion, the incumbent Contractor shall provide familiarization and allow the follow-on Contractor to observe monthly operations, facilities, work, equipment locations and reporting procedures on a non-interference basis.

3.23.8 The incumbent Contractor shall ensure network access is removed for those employees who do not intend to work for the new Contractor, upon completion of their employment.

3.24 Conformance with Environmental Management Systems

The Contractor shall perform work under this contract consistent with the relevant policy and objectives identified in the agency, organizational, or facility Environmental Management System (EMS) applicable for your contract. The Contractor shall perform work in a manner that conforms to all appropriate Environmental Management Programs and Operational Controls identified by the agency, organizational, or facility EMS, and provide monitoring and measurement information as necessary for the organization to address environmental performance relative to the environmental, energy, and transportation management goals.

3.24.1 In the event an environmental nonconformance or noncompliance associated with the contracted services is identified, the Contractor shall take corrective and/or preventative actions. In the case of a noncompliance, the Contractor shall respond and take corrective action immediately. In the case of a nonconformance, the Contractor shall respond and take corrective action based on the time schedule established by the EMS Site Coordinator. In addition, the Contractor shall ensure that their employees are aware of the roles and responsibilities identified by the environmental management system and how these requirements affect their work performed under this contract.

3.24.2 Upon contract award, the COR will notify the facility-level Environmental Management Systems Coordinator to arrange EMS training for appropriate staff. Thereafter, all on-site Contractor personnel shall complete yearly EPA sponsored environmental training specified for the type of work conducted on-site.

3.25 Participation in Government Activities

Contractor shall participate in various Government-initiated activities such as Continuous Process Improvement (CPI) initiatives, process identification and management, various meetings, safety programs related to work center hazards/Voluntary Protection Program (VPP) and similar activities as requested by the Government.

4.0 Services Summary

SS #	Performance Objective	PWS Section	Performance Threshold	Monitoring Method
1	**VTC/AV Maintenance Activity Report (MAR)** (CDRLA001)	1.1 2.3.1	• MAR shall include a list of all VTC/AV systems with operational and STIG-compliance status. • Report should contain a list of service calls and requests for support including Service Now ticket number(s) and organizations supported including training, • MAR will be submitted no later than the 5th business day of the month.	COR
3	**Staffing Roster** (CDRLA002)	1.2 3.8	• Within 10 business days of contract award, the contractor shall provide a list of all personnel who could be called upon to support this contract. • Contractor shall notify the Security Manager and COR, in writing, about changes to the staffing roster, including the addition of new personnel or removal of personnel, within five (5) business days of change.	Security Manager and COR
4	**User Documentation and Training** (CDRLA003)	1.3	• Contractor will coordinate with customer(s) to provide copies of user manuals, in digital format preferably, and to provide as-needed user training on the use of the system(s).	MAR
6	**Corrective Maintenance**	2.3.6 1.1	• Contractor shall respond to requests for corrective maintenance within identified response times. • Contractor shall include details about corrective maintenance requests and resolution as part of the MAR.	Service Now Reports MAR
7	**Security Requirements**	3.10 – 3.12	Contractors shall ensure compliance with all security requirements including, but not limited to: • DD254 • Security Clearance Investigations • Non-Disclosures	Security Manager COR
8	**Training**	3.19	Contractor shall ensure all personnel complete required training for access to the facilities and network.	75 ABW/SC Training Manager

ADDENDUM A: REFERENCES

AFPD 40-1 Health Promotion
AFPD 91-2 Safety Programs
AFI 10-245 Antiterrorism (AT)
AFI 16-1404 Air Force Information Security Program
AFI 40-101 Health Promotion
AFMAN 33-282 Computer Security (COMPUSEC)
DODD 5220.22-M National Industrial Security Program Operating Manual (NISPOM)
DODD 8500.01E Information Assurance
DODI 8500.2 Information Assurance Implementation
DODI 8510.01 DOD Information Assurance Certification and Accreditation Process (DIACAP)
DOD 8570.01-M Information Assurance Workforce Improvement Program
Committee on National Security Systems Instructions (CNSSI) 4009, National Information Assurance Glossary (available at http://www.cnss.gov/full-index.html)
Memorandum, Office of the Under Secretary of Defense, 1 April 2005, Subject: Facilitating Classified Visits within Department of Defense (available from the Government requiring agency) Memorandum, Office of Under Secretary of Defense, 5 December 2001, subject: Facilitating Necessary Access to NATO Classified Information (available from the Government requiring agency).

ADDENDUM B: ACRONYMS

ACRONYM	DEFINITION
APL	Approved Product List
AV	Audio-Visual
CAC	Common Access Card
CDRL	Contract Deliverables Requirements List
CIL	Critical Information List
CM	Counter Measures
COR	Contract Office Representative
CPI	Continuous Process Improvement
CTS	Certified Technology Specialist
DISA	Defense Information Systems Agency
DoD	Department of Defense
EOL	End of Life
FOD	Foreign Object Damage
FOIA	Freedom of Information Act
IAW	In Accordance With
JER	Joint Ethics Regulations
MAR	VTC/AV Maintenance Activity Report
OM	OPSEC Measures
OPSEC	Operation Security
PMI	Preventive Maintenance Inspections
PWS	Performance Work Statement
QCP	Quality Control Plan
SDC	Standard Desktop Configuration
STIG	Strategic Technical Implementation Guide
VPN	Virtual Private Network
VPP	Voluntary Protection Program
VTC	Video Teleconferencing