Statement of Work (SOW)

SECURE UNIFIED COMMUNICATIONS CONFERENCE SYSTEM (UCCS)

Buckley SFB - INTEGRATED OPERATIONS CENTER (IOC) AND CRISIS ACTION TEAM (CAT)

1.0 SCOPE AND MISSION

1.1 Scope

The Contractor shall provide, install, integrate, configure, test, train, document, and sustain a secure Unified Communications Conference System (UCCS) to support the Government's Integrated Operations Center (IOC) and Crisis Action Team (CAT) mission.

The UCCS shall provide secure, voice-centric conferencing and emergency communications capabilities supporting routine operations, contingency operations, crisis response, and emergency notification.

The solution shall integrate with the Government's existing Cisco Unified Communications Manager (CUCM) environment and shall support applicable Department of Defense (DoD) Assured Services SIP (AS-SIP), Defense Switched Network (DSN), Multi-Level Precedence and Preemption (MLPP), encryption, authentication, cybersecurity, and interoperability requirements.

The Government intends to acquire a complete, operationally ready solution. The Contractor shall provide all hardware, software, licenses, infrastructure, integration services, documentation, training, maintenance, and technical support necessary to satisfy the requirements of this SOW.

The Contractor shall provide a turnkey capability that does not require the Government to independently procure or provide infrastructure necessary for normal system operation, except for Government-furnished systems and services expressly identified in this SOW.

1.2 Mission

The UCCS shall support the IOC and CAT by providing a reliable and secure capability to:

- Establish and manage routine and emergency audio conferences.
- Rapidly assemble predefined emergency response groups.
- Provide secure conference communications during crisis and contingency operations.
- Support DoD priority communications and MLPP.
- Support secure communications through the Government's existing CUCM and approved voice infrastructure.
- Provide conference recording and post-incident audit capabilities when authorized.
- Operate continuously in support of 24/7/365 mission requirements.
- Minimize operator actions required to initiate emergency conferences.
- Provide rapid identification of participant connection status during emergency conference activation.

1.3 Vendor-Neutral Requirement

The Government is not specifying a particular manufacturer, product, proprietary architecture, or implementation methodology unless expressly identified as a Government-mandated interface, standard, or requirement.

The Contractor may quote:

- A dedicated physical/COTS appliance;
- A Contractor-provided virtualized architecture;
- A combination of physical and virtual components; or
- Another architecture that demonstrably satisfies all requirements of this SOW.

The Government will evaluate quoted solutions based on demonstrated compliance with:

- Mission capability;
- Functional requirements;
- CUCM/AS-SIP interoperability;
- Cybersecurity;
- Performance;
- Availability and resiliency;
- Infrastructure requirements;
- Implementation complexity;
- Training requirements;
- Sustainment requirements;
- Technical risk; and
- Total lifecycle cost.

2.0 APPLICABLE STANDARDS AND REQUIREMENTS

The Contractor shall comply with applicable versions of Government standards, policies, and technical requirements in effect during contract performance, including, as applicable:

- Department of Defense (DoD) Unified Capabilities requirements.
- Joint Interoperability Test Command (JITC) certification and interoperability requirements.
- DoD Assured Services SIP (AS-SIP) requirements.
- Defense Switched Network (DSN) requirements.
- Multi-Level Precedence and Preemption (MLPP) requirements.
- DoD Public Key Infrastructure (PKI) requirements.
- Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs).
- Risk Management Framework (RMF) requirements.
- Applicable DoD Chief Information Officer (CIO) cybersecurity policies.
- Federal Information Processing Standards (FIPS) requirements applicable to cryptographic modules.
- Applicable Government records, auditing, logging, and cybersecurity requirements.

The Contractor shall identify all certifications, approvals, validations, and technical standards applicable to the quoted solution.

2.1 JITC Certification and Interoperability

The Contractor shall provide evidence of applicable JITC certification or interoperability validation for the quoted product, software release, hardware configuration, and deployment architecture.

The Contractor shall identify:

- Certification or validation number.
- Applicable product/model.
- Tested software release.
- Tested hardware configuration.
- Tested architecture.
- Certification/validation date and status.
- Applicable interoperability capabilities.
- Restrictions or limitations.
- Differences between the certified/tested configuration and the configuration quoted to the Government.

If the quoted configuration differs from the configuration evaluated or certified by JITC or another applicable authority, the Contractor shall identify the differences and explain the potential impact on:

- Interoperability;
- Cybersecurity;
- Certification status;
- Performance;
- Availability; and
- Operational risk.

3.0 SYSTEM FUNCTIONAL REQUIREMENTS

The Contractor shall provide a UCCS capable of operating without continuous manual operator intervention or dedicated conference-bridge console management.

3.1 Conference Types

The UCCS shall support:

- Meet-Me (dial-in) conferences.
- Ad-hoc conferences.
- Scheduled conferences.
- Pre-programmed/preset conferences.
- Emergency conferences.
- Administrator-initiated conferences.
- Authorized user-initiated conferences.

The Contractor shall identify whether each conference type is a native system capability or requires an external application, service, license, or component.

3.2 Conference Administration

The system shall provide authorized administrators with the capability to:

- Create, modify, and delete conference profiles.
- Establish predefined conference groups.
- Configure conference access numbers and associated parameters.
- Establish authorized users and administrative roles.
- Configure conference security controls.
- Monitor active conferences.
- Terminate conferences when authorized.
- Review conference activity and audit records.
- Configure emergency response groups.

- Test emergency response groups without initiating an uncontrolled emergency notification.

The Contractor shall identify all administrative functions requiring privileged access and all functions requiring separate management systems or applications.

3.3 Automated Emergency Outbound Dialing

The UCCS shall provide an automated emergency outbound dialing capability to rapidly assemble predefined IOC/CAT response groups.

The system shall:

- Maintain administrator-configurable emergency response groups.
- Initiate automated outbound calls to predefined participants.
- Support simultaneous initiation of outbound calls to multiple predefined destinations.
- Automatically place successfully connected participants into the designated secure conference.
- Support multiple predefined response groups.
- Identify answered, busy, unreachable, and failed destinations.
- Support configurable retry behavior where available.
- Provide authorized personnel with the ability to activate emergency conferences rapidly.
- Maintain an auditable record of emergency conference activation and participant connection status.
- Support authorized modification and testing of emergency response groups.

The Contractor shall identify:

- Maximum destinations that may be dialed simultaneously.
- Maximum concurrent automated emergency outbound dialing operations.
- Maximum response-group size.
- Time required to initiate outbound calls.
- Time required to establish the conference.
- Retry capabilities.
- Busy/no-answer handling.
- Failed-destination handling.
- Participant status reporting.
- Third-party dependencies.
- Additional licensing requirements.
- External telecommunications services required.

The Government may establish minimum emergency dialing performance thresholds in the final requirements matrix.

3.4 Emergency Notification

Where required by the Government, the solution shall support emergency notification through approved communications methods.

The Contractor shall identify supported notification mechanisms, including, where available:

- Telephone/voice notification.
- SIP endpoints.
- DSN endpoints.
- Commercial telephone endpoints.
- SMS/text notification.
- Email notification.
- Other Government-approved notification mechanisms.

The Contractor shall identify which notification capabilities are:

1. Native to the quoted UCCS;
2. Provided through Contractor-supplied components;
3. Provided through third-party products or services; or
4. Dependent upon Government-furnished systems or services.

The Contractor shall identify all additional licensing, infrastructure, network connectivity, telecommunications services, and recurring fees required for each notification capability.

3.5 Recording

The UCCS shall support secure recording of authorized conferences.

The system shall provide:

- Administrator-controlled recording.
- Secure storage.
- Access control.
- Recording identification and metadata.
- Retrieval by authorized personnel.
- Audit logging.
- Configurable retention parameters.

The Contractor shall identify:

- Maximum recording capacity.
- Storage requirements.
- Recording format.
- Storage architecture.
- Encryption method.
- Retention limitations.
- Export capabilities.
- Additional licensing or infrastructure requirements.

3.6 Capacity

The system shall support the Government's required conference capacity without degradation of required voice quality, encryption, signaling, or mission functions.

The Contractor shall provide documented capacity for:

- Maximum simultaneous conferences.
- Maximum participants per conference.
- Maximum aggregate simultaneous participants.
- Maximum concurrent SIP sessions.
- Maximum concurrent automated emergency outbound dialing operations.
- Maximum simultaneous recordings.
- Maximum supported emergency response groups.

The Contractor shall distinguish between:

- Manufacturer maximum capacity;
- Recommended operational capacity;
- Capacity supported by the quoted configuration; and
- Capacity demonstrated during testing.

The Government will establish minimum capacity thresholds in the final requirements matrix.

4.0 CUCM, SIP, AND DSN INTEROPERABILITY

4.1 CUCM Integration

The UCCS shall integrate with the Government's existing Cisco Unified Communications Manager (CUCM) environment using a Government-approved SIP/AS-SIP architecture.

The Contractor shall not require replacement of the Government's CUCM environment unless specifically authorized by the Government.

The Contractor shall identify all required CUCM configuration changes, including, as applicable:

- SIP trunks.
- SIP profiles.
- Route patterns.
- Route groups.
- Route lists.
- Calling Search Spaces (CSS).
- Partitions.
- Device pools.
- Security profiles.
- Certificates.
- Codec configurations.
- Dial-plan changes.
- Media resources.
- Transcoding resources.
- Other required CUCM modifications.

The Contractor shall identify all CUCM licenses, feature licenses, or additional Government-side licensing required to implement the quoted solution.

4.2 Signaling

The system shall support applicable DoD AS-SIP requirements and shall provide secure SIP signaling using TLS where required by the Government's security architecture.

The Contractor shall document:

- SIP signaling architecture.
- SIP signaling paths.
- Required ports.
- TLS versions.
- Supported cipher suites.
- Certificate requirements.
- Authentication requirements.
- SIP trunk requirements.
- Dependencies on SBCs or other intermediary systems.

4.3 Media Security

The UCCS shall support Secure Real-time Transport Protocol (SRTP) for protection of conference media where required by the Government.

The Contractor shall identify:

- Supported SRTP profiles.
- Supported cryptographic algorithms.
- Key exchange mechanisms.
- Media security requirements.
- CUCM interoperability requirements.
- Limitations on encrypted conference participation.
- Scenarios in which media may become unencrypted.

4.4 Session Controller Architecture

The Contractor shall identify the quoted role of:

- CUCM.
- Session Controllers.
- Local Session Controllers (LSC).
- Session Border Controllers (SBC), where applicable.
- SIP trunks.
- Conference bridges.
- Gateways.
- Other intermediary components.

The Contractor shall not assume that CUCM is the LSC unless that architecture is validated and approved by the Government.

4.5 DTMF

The system shall support standard Dual-Tone Multi-Frequency (DTMF) signaling required for:

- Conference access.
- Participant authentication.
- Conference control.
- Participant management.
- Automated emergency outbound dial activation.
- Other required conference functions.

The Contractor shall identify the supported DTMF signaling method(s) and any interoperability limitations.

4.6 Codec Support

The system shall support the voice codecs required by the Government's existing CUCM, AS-SIP, and DSN environment.

The Contractor shall identify all supported codecs, including, where applicable, G.711, G.729a, and other codecs supported by the quoted solution.

The Contractor shall identify any codec limitations associated with:

- Secure media.
- Conference bridging.
- Recording.
- Transcoding.
- MLPP.
- DSN interoperability.

5.0 MLPP AND PRIORITY COMMUNICATIONS

The UCCS shall support applicable DoD Multi-Level Precedence and Preemption (MLPP) requirements.

The Contractor shall demonstrate:

- Priority assignment.
- Precedence handling.
- Call queuing.
- Preemption.
- Behavior during resource exhaustion.
- Interaction with CUCM.
- Interaction with AS-SIP.
- Interaction with DSN.
- Behavior of active conferences during MLPP events.
- Behavior of automated emergency outbound dialing during MLPP events.

The Contractor shall document any limitations regarding MLPP treatment of:

- Active conferences.
- Conference participants.
- Automated emergency outbound dialing operations.
- Recorded conferences.
- Conference resources.
- Emergency notification operations.

The Contractor shall identify whether MLPP functionality is native to the UCCS or dependent upon CUCM, a Session Controller, DSN infrastructure, or another component.

6.0 INFRASTRUCTURE AND HOSTING

6.1 Government-Furnished Virtualization

The Government does not currently possess an enterprise virtualization environment available for this requirement.

The Contractor shall therefore provide all infrastructure necessary to host and operate the quoted solution.

The Contractor shall not assume the availability of Government-furnished:

- Virtual machines.
- Hypervisors.
- Virtualization hosts.
- Storage.
- Backup infrastructure.
- Hardware management systems.
- Application hosting platforms.

6.2 Contractor-Provided Infrastructure

The Contractor shall provide, install, configure, secure, maintain, and support all infrastructure necessary for the quoted UCCS solution, including, as applicable:

- Physical servers.
- Virtualization hosts.
- Hypervisor software.
- Operating systems.
- Application software.
- Storage.
- Network interfaces.
- Backup systems.
- High-availability components.
- Management systems.
- Required licenses.
- Required support agreements.
- Hardware warranties.
- Replacement components.

The Contractor shall identify whether the quoted UCCS requires:

1. Dedicated physical hardware;
2. Contractor-provided virtualization infrastructure;
3. A combination of physical and virtual components; or
4. Other infrastructure.

6.3 Physical Deployment Option

Where a physical appliance or dedicated server architecture is quoted, the Contractor shall identify:

- Server model and configuration.
- Processor requirements.
- Memory requirements.
- Storage requirements.
- RAID configuration.
- Network interfaces.
- Power requirements.
- Rack requirements.
- Environmental requirements.
- Hardware redundancy.
- Hardware lifecycle.
- Warranty.
- Replacement-part availability.

6.4 Virtualized Deployment Option

Where a virtualized architecture is quoted, the Contractor shall provide all required virtualization infrastructure unless otherwise identified as Government-furnished.

The Contractor shall identify:

- Hypervisor.
- Host requirements.
- VM requirements.
- vCPU requirements.
- Memory requirements.
- Storage requirements.
- Network requirements.
- High-availability requirements.
- Backup requirements.
- Hypervisor licensing.
- Operating-system licensing.
- Application licensing.

- Security requirements.

The Contractor shall identify whether the quoted configuration is included within the applicable JITC-certified or otherwise validated architecture.

6.5 Infrastructure Dependencies

The Contractor shall identify all infrastructure, software, services, licenses, network connectivity, telecommunications services, and third-party components required for full operation of the quoted UCCS.

The Contractor shall identify any component that must be provided, configured, licensed, or maintained by the Government.

The Government will not consider a solution fully compliant if required infrastructure or dependencies are omitted from the quote and subsequently identified as necessary for normal operation.

6.6 Complete Solution Pricing

The Contractor shall separately identify the acquisition and recurring costs associated with:

- UCCS software.
- Hardware.
- Virtualization/hypervisor licensing.
- Operating-system licensing.
- Storage.
- Backup.
- Networking.
- Required third-party software.
- Required third-party hardware.
- Installation.
- Integration.
- Testing.
- Training.
- Security/RMF support.
- Maintenance.
- Technical support.
- Hardware replacement.
- Software upgrades.
- Technology refresh.

The Contractor shall provide sufficient information for the Government to calculate the total five-year lifecycle cost of the quoted solution.

7.0 AVAILABILITY, HIGH AVAILABILITY, AND RESILIENCY

7.1 Operational Availability

The UCCS shall support continuous IOC/CAT operations 24 hours per day, 7 days per week, 365 days per year.

The Contractor shall quote an architecture capable of meeting a minimum system availability of

percent.

The Contractor shall identify all planned and unplanned availability exclusions.

7.2 High Availability

The UCCS shall incorporate redundancy appropriate to the quoted architecture.

The Contractor shall identify:

- Application redundancy.
- Hardware redundancy.
- Processing redundancy.
- Storage redundancy.
- Network redundancy.
- Power redundancy.
- Conference bridge redundancy.
- Failure detection.
- Automatic recovery.
- Manual recovery requirements.

7.3 Failover

The Contractor shall demonstrate system behavior during:

- Single-node failure.
- Application failure.
- Hardware failure.
- Network failure.
- Storage failure.
- Power interruption where applicable.
- CUCM/SIP connectivity failure.

The Contractor shall identify the expected service interruption associated with each failure condition.

7.4 Active Conference Preservation

The Contractor shall identify whether active conferences are:

- Preserved without interruption;
- Preserved with a brief interruption;
- Automatically re-established; or
- Terminated and manually re-established.

The Contractor shall demonstrate the actual behavior during acceptance testing.

7.5 Backup

The Contractor shall implement automated backup of required system configuration and data.

The backup solution shall support:

- Scheduled backups.
- Configuration backup.
- Database backup where applicable.
- Secure backup storage.
- Backup retention.
- Backup verification.
- Restoration testing.

7.6 Disaster Recovery

The Contractor shall provide a Disaster Recovery (DR) plan identifying:

- Recovery Time Objective (RTO).
- Recovery Point Objective (RPO).
- Recovery procedures.
- Backup requirements.
- Restoration procedures.
- Required replacement hardware.
- Required licenses.
- System dependencies.
- Government dependencies.

The Government will establish minimum RTO/RPO thresholds in the final requirements matrix.

8.0 CYBERSECURITY

8.1 Risk Management Framework

The Contractor shall support the Government's applicable Risk Management Framework (RMF) and Authority to Operate (ATO) requirements.

The Contractor shall provide technical documentation and security artifacts necessary to support the Government's cybersecurity authorization process.

8.2 STIG Compliance

All applicable Contractor-provided operating systems, applications, virtualization components, and infrastructure shall be hardened in accordance with applicable DISA STIGs.

The Contractor shall provide:

- Applicable STIG identification.
- STIG checklists.
- Security configuration documentation.
- Vulnerability scan results.
- Remediation status.
- POA&M support where applicable.
- Configuration baselines.

8.3 Product Certification and Approval

The Contractor shall identify all applicable DoD product certifications, approvals, and interoperability validations associated with the quoted solution.

The Contractor shall provide:

- Certification or approval name.
- Certification number.
- Certified software version.
- Certified hardware configuration.
- Certified deployment architecture.
- Certification status.
- Certification limitations.
- Differences between the certified configuration and quoted deployment.

8.4 Cryptography

Cryptographic mechanisms used to protect Government information shall comply with applicable FIPS validation requirements and DoD cybersecurity policy.

The Contractor shall identify:

- Cryptographic modules.
- FIPS validation numbers.
- Encryption algorithms.
- Key management.
- Certificate requirements.
- TLS implementation.
- SRTP implementation.

8.5 PKI and CAC Authentication

The system shall support Government-approved DoD PKI authentication for administrative access and other functions requiring strong authentication.

The Contractor shall identify:

- Certificate requirements.
- Certificate authorities.
- Certificate enrollment.
- Certificate validation.
- Certificate revocation checking.
- Certificate renewal.
- Administrative authentication.
- CAC authentication.

8.6 Logging and Auditing

The system shall provide security and operational logging sufficient to support Government monitoring and audit requirements.

The Contractor shall identify support for:

- Syslog.
- Security events.
- Administrative activity.
- Authentication events.
- Conference activity.

- Automated emergency outbound dialing activity.
- Configuration changes.
- System failures.

8.7 Vulnerability Management

The Contractor shall provide timely security updates and patches for Contractor-provided components.

The Contractor shall:

- Monitor applicable vulnerabilities.
- Notify the Government of vulnerabilities affecting the system.
- Provide remediation recommendations.
- Provide security patches.
- Identify vulnerabilities that cannot be remediated.
- Support Government vulnerability scanning.
- Support applicable POA&M activities.

9.0 IMPLEMENTATION AND INTEGRATION

9.1 Implementation Planning

The Contractor shall develop an Implementation and Integration Plan addressing:

- System architecture.
- Site preparation.
- Hardware installation.
- Software installation.
- Network integration.
- CUCM integration.
- Security configuration.
- PKI integration.
- Testing.
- Training.
- Migration.
- Cutover.
- Rollback.

9.2 Installation

The Contractor shall:

- Install Contractor-provided hardware.

- Install required software.
- Configure infrastructure.
- Configure network connectivity.
- Configure security.
- Configure CUCM integration.
- Configure conference services.
- Configure emergency response groups.
- Configure recording.
- Configure backup.

9.3 CUCM Integration

The Contractor shall coordinate with Government network and voice engineers to implement and validate the approved CUCM/SIP integration.

The Contractor shall be responsible for identifying all required Government-side configuration changes and shall provide step-by-step implementation procedures.

9.4 Migration

Where replacing or transitioning from an existing conferencing capability, the Contractor shall develop and execute an approved migration plan addressing:

- Conference numbers.
- User accounts.
- Conference profiles.
- Preset conferences.
- Emergency response groups.
- Recording requirements.
- Administrative configurations.
- Security configurations.
- Operational procedures.

9.5 Cutover

The Contractor shall perform production cutover only after Government approval of:

- Implementation plan.
- Test results.
- Security requirements.
- MOP.
- Training.
- Rollback procedures.

9.6 Rollback

The Contractor shall provide a documented rollback procedure capable of restoring the pre-cutover operational state if acceptance criteria are not met.

10.0 TESTING AND ACCEPTANCE

10.1 Test Plan

The Contractor shall develop a System Test and Acceptance Plan identifying test objectives, procedures, expected results, dependencies, Government participation, and acceptance criteria.

10.2 Factory Acceptance Testing

Where applicable, the Contractor shall conduct Factory Acceptance Testing (FAT) prior to production deployment.

FAT shall verify:

- Core conference functionality.
- Automated emergency outbound dialing.
- Recording.
- MLPP.
- TLS.
- SRTP.
- Capacity.
- Backup.
- Restoration.
- High availability.

10.3 Site Acceptance Testing

The Contractor shall conduct Site Acceptance Testing (SAT) following installation.

SAT shall verify:

- CUCM integration.
- AS-SIP interoperability.
- DSN interoperability.
- Dial plan.
- PKI.
- TLS.
- SRTP.

- MLPP.
- Automated emergency outbound dialing.
- Emergency notification.
- Recording.
- Failover.
- Backup and restoration.
- Security configuration.

10.4 Performance Testing

The Contractor shall demonstrate required system capacity under representative IOC/CAT loads.

Testing shall include, as applicable:

- Concurrent conferences.
- Concurrent participants.
- Concurrent SIP sessions.
- Concurrent automated emergency outbound dialing.
- Recording load.
- Emergency conference activation.

10.5 Failure Testing

The Contractor shall demonstrate system behavior during:

- Single-node failure.
- Application failure.
- Hardware failure.
- Network interruption.
- Power interruption where applicable.
- Storage failure where applicable.
- CUCM/SIP connectivity failure.
- Restoration following outage.

10.6 MLPP Testing

The Contractor shall demonstrate required MLPP behavior through the Government's designated CUCM/AS-SIP environment.

Testing shall verify:

- Priority assignment.
- Precedence.

- Queuing.
- Preemption.
- Conference interaction.
- Resource exhaustion behavior.
- Automated emergency outbound dialing interaction.

10.7 Automated Emergency Outbound Dialing Testing

The Contractor shall demonstrate:

- Emergency group configuration.
- Simultaneous outbound dialing.
- Automatic conference joining.
- Busy handling.
- No-answer handling.
- Failed-number handling.
- Retry behavior.
- Participant status.
- Audit logging.
- Operator activation procedure.

10.8 Operational Acceptance

Final operational acceptance shall require:

- Successful completion of required FAT/SAT testing.
- Successful CUCM/AS-SIP interoperability testing.
- Successful security validation.
- Successful MLPP demonstration.
- Successful automated emergency outbound dialing demonstration.
- Successful failover demonstration.
- Completion of required training.
- Delivery and Government acceptance of required documentation.
- Resolution or Government acceptance of all critical deficiencies.

11.0 TRAINING

11.1 Administrator Training

The Contractor shall provide administrator training covering:

- System administration.
- User administration.
- Conference configuration.
- Emergency response group administration.

- Automated emergency outbound dialing.
- Security configuration.
- PKI/certificate management.
- Logging.
- Backup and restoration.
- Troubleshooting.
- Maintenance.
- Software upgrades.

11.2 IOC/CAT User Training

The Contractor shall provide training covering:

- Meet-Me conferences.
- Ad-hoc conferences.
- Scheduled conferences.
- Preset conferences.
- Emergency conference activation.
- Automated emergency outbound dialing.
- Conference controls.
- Participant management.
- Emergency operating procedures.
- Troubleshooting.

11.3 Training Materials

The Contractor shall provide:

- Instructor materials.
- Student materials.
- Administrator guide.
- User guide.
- Quick-reference guides.
- Emergency operating procedures.
- Training recordings where applicable.

11.4 Training Completion

Required training shall be completed prior to operational acceptance unless otherwise approved by the Government.

12.0 SUSTAINMENT AND SUPPORT

12.1 Lifecycle Sustainment

The Contractor shall provide lifecycle sustainment for the period of performance specified in the contract.

12.2 Software Maintenance

The Contractor shall provide:

- Bug fixes.
- Security updates.
- Maintenance releases.
- Major software releases where included in the contract.
- Technical advisories.
- Certification-impact notifications.

12.3 JITC and Certification Management

The Contractor shall notify the Government of changes that may affect:

- JITC certification.
- DoD approval.
- AS-SIP interoperability.
- Cybersecurity authorization.
- STIG compliance.
- CUCM interoperability.

The Contractor shall not implement changes that materially affect required certifications or authorizations without Government approval.

12.4 Technical Support

The Contractor shall provide 24/7/365 Tier 2 and Tier 3 technical support for Priority 1 system outages.

The Contractor shall provide defined:

- Time to acknowledge.
- Time to respond.
- Time to restore.
- Escalation procedures.
- Vendor escalation procedures.

Specific SLA thresholds shall be established in the applicable contract section or Performance Requirements Summary.

12.5 Hardware Support

For Contractor-provided physical infrastructure, the Contractor shall provide replacement components and hardware support consistent with Government-established service levels.

The Contractor shall identify:

- Warranty period.
- Replacement timeframe.
- Spare-parts strategy.
- End-of-life notification.
- Technology refresh process.

12.6 Configuration Management

The Contractor shall maintain an approved configuration baseline for the UCCS.

The Contractor shall document:

- Hardware configuration.
- Software versions.
- Firmware versions.
- Configuration changes.
- Security configuration.
- Certificates.
- Network interfaces.
- CUCM integration configuration.

13.0 DOCUMENTATION AND DELIVERABLES

The Contractor shall provide, at a minimum:

Deliverable	Description
System Design Document	Architecture, components, interfaces, data flows
Implementation Plan	Installation, integration, configuration, migration
Method of Procedure (MOP)	Detailed production implementation procedures
Test Plan	FAT, SAT, performance, failover, security testing

Test Report	Results, deficiencies, corrective actions
Security Configuration Guide	Security architecture and hardening
STIG Artifacts	Applicable STIG checklists and scan results
RMF/ATO Artifacts	Applicable cybersecurity documentation
Training Materials	Administrator and user training
As-Built Drawings	Final architecture and network diagrams
Interface Control Documentation	CUCM/SIP/AS-SIP interfaces
O&M Manual	Routine operation and maintenance
Backup/Restore Plan	Backup and restoration procedures
Disaster Recovery Plan	DR architecture and recovery procedures
Configuration Baseline	Approved production configuration
PKI Documentation	Certificate and PKI requirements
License Documentation	All licenses and entitlements
Hardware Documentation	Equipment specifications and warranties
JITC Documentation	Applicable certification/validation evidence
Software Version Matrix	Approved software and firmware versions
Dependency Matrix	Government, Contractor, and third-party dependencies

All final documentation shall reflect the actual production configuration.

14.0 QUOTE TECHNICAL RESPONSE REQUIREMENTS

Each offeror shall provide sufficient technical information for the Government to independently evaluate compliance with this SOW.

14.1 Architecture

The offeror shall provide:

- Quoted architecture.
- Physical/virtual deployment.
- System components.
- Network architecture.
- CUCM integration architecture.
- SIP/AS-SIP architecture.
- Security architecture.
- HA/DR architecture.
- Infrastructure dependencies.

14.2 Functional Compliance Matrix

The offeror shall provide a compliance matrix identifying each SOW requirement as:

- Compliant;
- Compliant with configuration;
- Compliant with additional component;
- Compliant with third-party dependency;
- Partially compliant; or
- Non-compliant.

The offeror shall provide supporting documentation for each exception or dependency.

14.3 Capacity

The offeror shall provide documented maximum and recommended capacities for:

- Concurrent conferences.
- Participants per conference.
- Aggregate participants.
- SIP sessions.
- Automated emergency outbound dialing.
- Recording.
- Emergency response groups.

14.4 Certification

The offeror shall provide applicable:

- JITC certifications.
- Certification reports.
- DoD approvals.
- FIPS validations.
- STIG information.
- Other applicable interoperability certifications.

14.5 Interoperability

The offeror shall provide evidence of successful interoperability with:

- Cisco CUCM.
- AS-SIP.
- DSN.
- MLPP.
- TLS/SRTP.
- Government PKI.

The offeror shall identify all limitations, required third-party components, or additional infrastructure.

14.6 Infrastructure

The offeror shall identify all Contractor-furnished:

- Servers.
- Storage.
- Virtualization.
- Hypervisor.
- Operating systems.
- Networking.
- Backup.
- HA components.
- Licenses.

14.7 Training

The offeror shall identify:

- Training duration.
- Number of personnel supported.
- Training location.
- Required prerequisites.
- Administrator training.
- User training.

14.8 Transition

The offeror shall provide a transition approach identifying:

- Implementation duration.
- Engineering requirements.
- Government support requirements.
- Testing.

- Migration.
- Cutover.
- Training.
- Risk mitigation.

15.0 TOTAL COST OF OWNERSHIP

The Contractor shall provide pricing sufficient for the Government to evaluate total lifecycle cost.

Pricing shall separately identify, at a minimum:

1. UCCS software licenses.
2. Hardware.
3. Virtualization infrastructure.
4. Hypervisor licensing.
5. Operating-system licensing.
6. Storage.
7. Backup.
8. Network infrastructure.
9. Required third-party components.
10. Installation.
11. Engineering integration.
12. CUCM integration.
13. Cybersecurity/RMF support.
14. Testing.
15. Training.
16. Documentation.
17. Software maintenance.
18. Hardware maintenance.
19. Technical support.
20. Hardware replacement.
21. Technology refresh.
22. Certification maintenance.
23. Optional capabilities.

The Contractor shall provide a five-year total lifecycle cost.

The offeror shall identify all assumptions used to calculate quoted pricing.

The Government shall consider total lifecycle cost rather than acquisition price alone.

16.0 GOVERNMENT-FURNISHED INFORMATION AND EQUIPMENT

The Government anticipates providing:

- Existing CUCM environment.
- Existing Government voice/network connectivity.
- Required network access.
- Government technical points of contact.
- Applicable Government security policies.
- Required interface and configuration information.
- Government-furnished telephone/voice services as identified in the contract.

The Government does not currently provide an enterprise virtualization environment for this requirement.

The Contractor shall identify all additional Government-furnished equipment, information, services, licenses, or infrastructure required to operate the quoted solution.

Any Government dependency not expressly identified in the Contractor's quote shall be considered Contractor responsibility unless subsequently approved by the Government.

17.0 CONTRACTOR-FURNISHED EQUIPMENT AND SERVICES

Except where expressly identified as Government Furnished Equipment or Information, the Contractor shall provide all equipment, software, licenses, infrastructure, labor, tools, documentation, training, maintenance, and services necessary to satisfy the requirements of this SOW.

The Contractor shall be responsible for ensuring that all Contractor-furnished components are compatible with the quoted UCCS architecture and supported for the required period of performance.

18.0 SERVICE LEVEL REQUIREMENTS

The Contractor shall meet Government-established service levels for:

- System availability.
- Priority 1 response.
- Priority 1 restoration.
- Security vulnerability remediation.

- Hardware replacement.
- Technical support.
- Incident escalation.
- Software notification.
- Certification-impact notification.

Specific numerical Service Level Agreement (SLA) thresholds shall be established in the applicable contract section or Performance Requirements Summary (PRS).

At a minimum, the Contractor shall maintain documented procedures for measuring and reporting:

- Availability.
- Outages.
- Incident response.
- Restoration.
- Security remediation.
- Hardware failures.
- Software defects.

19.0 PERFORMANCE MONITORING AND REPORTING

The Contractor shall provide periodic reporting sufficient for the Government to assess system performance and sustainment.

Reports shall include, as applicable:

- System availability.
- Outages.
- Incident volume.
- Priority 1 incidents.
- Response times.
- Restoration times.
- Security vulnerabilities.
- Patch status.
- Hardware failures.
- Software defects.
- Certification status.
- Configuration changes.
- Capacity utilization.
- Backup status.
- DR test results.

The Contractor shall immediately notify the Government of conditions that materially affect mission availability, cybersecurity, interoperability, or certification status.

20.0 GOVERNMENT EVALUATION APPROACH

The Government intends to evaluate quoted solutions based upon demonstrated ability to satisfy IOC/CAT mission requirements while minimizing total lifecycle cost and implementation risk.

Evaluation factors may include:

Evaluation Area	Considerations
Mission Capability	Conference, emergency, automated outbound dialing, MLPP, recording
Emergency Response	Speed, automation, group management, participant status
Interoperability	CUCM, AS-SIP, DSN, PKI, SIP
Security	JITC, RMF, STIG, FIPS, encryption
Capacity	Conferences, participants, SIP sessions, emergency dialing
Resiliency	HA, failover, backup, DR
Infrastructure	Physical/virtual architecture and complexity
Implementation	Schedule, migration, integration risk
Training	Government training burden
Sustainment	Support, lifecycle, upgrades
Technical Risk	Dependencies, proprietary components, certification risk
Government Burden	Government engineering, infrastructure, administration
Lifecycle Cost	Acquisition plus five-year sustainment
Vendor Dependency	Proprietary components and long-term lock-in
Certification Risk	Difference between certified and quoted configurations

The Government may require offerors to demonstrate selected capabilities through technical demonstrations for proof-of-capability.

21.0 REQUIREMENTS TRACEABILITY AND COMPLIANCE

The Contractor shall maintain a requirements traceability matrix linking each SOW requirement to:

- Quoted system component.
- Software version.
- Hardware configuration.
- Applicable license.
- Applicable certification.
- Test procedure.
- Acceptance criterion.
- Supporting documentation.

The Contractor shall update the requirements traceability matrix following:

- Configuration changes.
- Software upgrades.
- Hardware changes.
- Certification changes.
- Security changes.
- Major maintenance activities.

The final approved requirements traceability matrix shall become part of the system baseline documentation.

22.0 GOVERNMENT MINIMUM PERFORMANCE REQUIREMENTS

The Government shall establish final numerical thresholds for the following requirements prior to solicitation or contract award:

Requirement	Government Threshold
Concurrent conferences	TBD
Participants per conference	TBD

Aggregate concurrent participants	TBD
Concurrent SIP sessions	TBD
Concurrent automated outbound calls	TBD
Emergency response group size	TBD
Emergency call initiation time	TBD
Emergency conference establishment time	TBD
System availability	TBD
Maximum planned outage	TBD
Maximum unplanned outage	TBD
Priority 1 response	TBD
Priority 1 restoration	TBD
RTO	TBD
RPO	TBD
Hardware replacement	TBD
Security vulnerability remediation	TBD

The Government shall establish these thresholds based on IOC/CAT mission requirements, existing CUCM capacity, DSN/AS-SIP requirements, operational staffing, expected conference utilization, and available funding.

23.0 REQUIRED VENDOR DISCLOSURES

Each offeror shall disclose all conditions that could materially affect Government acquisition, implementation, operation, or sustainment of the quoted solution.

At a minimum, the offeror shall identify:

- Required Government infrastructure.
- Required Government licenses.

- Required CUCM modifications.
- Required CUCM licenses.
- Required SBCs.
- Required gateways.
- Required third-party products.
- Required telecommunications services.
- Virtualization requirements.
- Physical hardware requirements.
- Software dependencies.
- Cloud dependencies.
- Certification dependencies.
- JITC limitations.
- Cybersecurity dependencies.
- Proprietary components.
- Training requirements.
- Specialized personnel requirements.
- Software upgrade requirements.
- Hardware refresh requirements.
- End-of-life considerations.
- Recurring licensing.
- Recurring support costs.

Failure to identify a required dependency may be considered during technical and price evaluation.

24.0 TRANSITION AND OPERATIONAL READINESS

The Contractor shall transition the UCCS into operational service without adversely affecting existing Government voice services.

The Contractor shall provide:

- Transition plan.
- Risk register.
- Implementation schedule.
- Site preparation plan.
- Installation plan.
- Integration plan.
- Testing plan.
- Training plan.
- Cutover plan.
- Rollback plan.

- Operational readiness assessment.

Prior to operational acceptance, the Contractor shall demonstrate that:

1. The system is installed and operational.
2. Required CUCM integration is complete.
3. Required security controls are implemented.
4. Required certifications/validations are documented.
5. Required conference functions operate correctly.
6. Automated emergency outbound dialing operates correctly.
7. MLPP operates correctly.
8. Required recording capability operates correctly.
9. Required failover capability operates correctly.
10. Required documentation has been delivered.
11. Required personnel have completed training.
12. No unresolved critical deficiency prevents mission operation.

25.0 FINAL OPERATIONAL ACCEPTANCE

Final Operational Acceptance shall occur only after the Government determines that the UCCS satisfies the applicable SOW requirements and approved acceptance criteria.

The Contractor shall correct all deficiencies identified during acceptance testing.

Critical deficiencies affecting:

- Emergency communications;
- Secure communications;
- CUCM interoperability;
- AS-SIP interoperability;
- DSN interoperability;
- MLPP;
- Automated emergency outbound dialing;
- Cybersecurity;
- System availability; or
- Mission-critical conference functionality

shall be resolved prior to final operational acceptance unless specifically waived in writing by the Government.

Upon acceptance, the Contractor shall provide the Government with the final:

- As-built configuration.

- Requirements traceability matrix.
- System architecture.
- Configuration baseline.
- Security baseline.
- Software/firmware version matrix.
- License inventory.
- Hardware inventory.
- O&M documentation.
- Backup/DR documentation.
- Training documentation.
- Certification documentation.
- Warranty/support documentation.

26.0 PERIOD OF PERFORMANCE

The Contractor shall provide services for:

- Base Period:
- Option Period 1:
- Option Period 2:
- Option Period 3:
- Option Period 4:

The Contractor shall maintain the UCCS in a fully operational and supported condition throughout the period of performance.

27.0 PLACE OF PERFORMANCE

Primary performance shall occur at the Government-designated IOC/CAT facility.

Contractor personnel may perform engineering, technical support, monitoring, maintenance, and other approved activities remotely when authorized by the Government and consistent with applicable security requirements.

Installation, testing, training, maintenance, and other activities requiring physical access shall be performed at the Government-designated site.

28.0 CONTRACTOR PERSONNEL

The Contractor shall provide qualified personnel necessary to perform all required services.

Personnel shall possess the technical qualifications necessary to:

- Administer the quoted UCCS.
- Integrate the system with CUCM.
- Configure SIP/AS-SIP.
- Troubleshoot secure voice communications.
- Support MLPP.
- Perform system maintenance.
- Support cybersecurity requirements.
- Perform backup and restoration.
- Troubleshoot hardware and software.
- Support emergency conference operations.

The Contractor shall identify specialized manufacturer certifications or training required to support the quoted system.

29.0 GOVERNMENT ENGINEERING BURDEN

The quoted solution shall minimize Government engineering and administrative burden.

The Contractor shall identify the estimated Government labor required for:

- Initial installation.
- CUCM integration.
- Network integration.
- Security authorization.
- Testing.
- Training.
- Routine administration.
- Software upgrades.
- Hardware replacement.
- Troubleshooting.
- Technology refresh.

The Government will consider required Government labor and infrastructure as part of total lifecycle cost and technical-risk evaluation.

30.0 TOTAL SOLUTION REQUIREMENT

The Contractor shall provide a complete and operationally ready UCCS capability satisfying the IOC/CAT mission requirements described in this SOW.

The Government will evaluate:

- Mission capability;
- Emergency response capability;
- Secure voice interoperability;
- MLPP;
- CUCM integration;
- JITC/DoD interoperability;
- Cybersecurity;
- Physical and virtual infrastructure requirements;
- Implementation complexity;
- Training requirements;
- Government engineering burden;
- Sustainment requirements;
- Technical risk;
- Vendor dependencies; and
- Total lifecycle cost.

The Contractor shall not require the Government to independently procure or provide infrastructure, software, licenses, services, or specialized components necessary to operate the quoted UCCS unless those requirements are expressly identified in the Contractor's quote and accepted by the Government.

The quoted solution shall provide the IOC/CAT with a secure, reliable, maintainable, and sustainable conferencing capability capable of supporting routine, contingency, and crisis operations throughout the period of performance.