AIR FORCE RESEARCH LABORATORY
ROME RESEARCH SITE
ROME, NEW YORK

STATEMENT OF WORK

FOR

COUNTER SMALL UNMANNED AIRCRAFT SYSTEMS (C-sUAS)

PCSN G-9-2307

21 NOV 2019

(Solicitation Number FA8750-20-R-1000)

DRAFT

TABLE OF CONTENTS

Section	Title	Page
1.0	OBJECTIVE	3
2.0	SCOPE	3
3.0	BACKGROUND	4
4.0	TECHNICAL REQUIREMENTS	5

DRAFT

1.0 OBJECTIVE

1.1 The objective of this effort is to provide a focused yet flexible, rapid, agile contracting vehicle between Air Force Research Laboratory, its Products Centers, and the Operational Community to support rapid research, development, prototyping, demonstration, evaluation, and transition of Counter small Unmanned Aircraft System (C-sUAS) capabilities. These capabilities are to be used in combating Commercial Off-The-Shelf (COTS) small Unmanned Aircraft Systems (sUAS)—and others leveraging COTS technology—presently being used by our adversaries in asymmetric warfare against U.S. military personnel and materiel. Emphasis will be placed on: a) development of technology capability solutions that address specific user requirements; b) delivery of prototype technologies for evaluation and feedback in the context of the user's operational environment; and c) provision of a mechanism for user acquisition of limited product quantities required for operational introduction of technologies.

2.0 SCOPE

2.1 The scope of this effort is to perform multiple activities necessary to achieve AFRL's vision of superiority in C-sUAS Science and Technology (S&T). This includes activities for rapid development, design, prototyping, enhancements, demonstration, scenario development, experimentation & evaluation, integration, testing, technical installation, transition and support through initial operations of C-sUAS technologies, which enable Global Vigilance, Global Reach, and Global Power in air, space, and cyberspace for C-sUAS operations. The primary goals are three-fold:

2.1.1 Develop new C-sUAS S&T capabilities and prototype solutions that can meet mission requirements and fill technology gaps across the entire C-sUAS kill-chain to include D5 effects (i.e. deceive, disrupt, deny, degrade, and destroy)

2.1.2 Demonstrate C-sUAS prototypes employing multiple mitigation techniques in a cooperative fashion that are able to achieve results in an automated and/or autonomous manner

2.1.3 Mature specific technological developments to mitigate multiple sUAS threats simultaneously, particularly enhancements of emerging baseline capabilities by AFLCMC, SBIRs, and industry in general.

DRAFT

2.2 Research and Development (R&D) in the following areas pertaining to C-sUAS include: analysis of Electromagnetic Spectrum (EMS) signals and signatures; developing detection, location, and identification techniques; developing link access techniques; cyberspace Intelligence, Surveillance, and Reconnaissance (ISR); development of cyberspace and EMS-enabled cyberspace countermeasures; integration of C-sUAS components and technologies; Command and Control (C2) using open architecture solutions; automation of capabilities; autonomy; prototyping; and demonstration.

2.3 R&D of cyberspace and cyber-enabled countermeasures (aka effects) that can be used as part of a C-sUAS dynamic kill chain are within scope. These efforts may employ blue-force sUAS in any part of the kill chain. Some of these EMS or EMS-enabled cyberspace measures could be classified and will be handled in accordance with the applicable Security Classification Guide (SCG).

3.0 BACKGROUND

3.1 The challenge of detecting, locating, and countering COTS sUAS and related technologies has become a dynamic and growing endeavor – it represents a global threat to US and allied forces. Of note, ISIS has successfully deployed these systems for both ISR and kinetic attacks via UAS-carried improvised explosive devices. Peer adversaries can field stealthy, more capable UAS and are continuing to improve their technologies. Moreover, advanced militaries are testing the use of swarms of unmanned aerial vehicles (UAVs) which are autonomous, distributed, collaborative systems made up of many small, cheap, unmanned aircrafts. The challenge of detecting and countering small UAS and sUAS swarms is particularly acute.

3.2 The US must develop superior technologies for the detection and countering of sUAS and sUAS swarms. These technologies must be advanced and include prospects for improvements in size, weight, power and performance as well as cost to develop and prove viable approaches to counter sUAS. Lastly, the US must be strategically positioned to rapidly respond to the dynamic and diverse sUAS threat to US personnel, equipment, and interests across the spectrum of local, regional and global threats.

3.3 Reference documents

3.3.1 Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated*

Terms, 12 April 2001 (as amended through 15 February 2016)

3.3.2 Air Force Research Laboratory, Mitigation of Small Unmanned Aircraft Systems (MsUAS) Security Classification Guide Revision 1, 20 Nov 2018

4.0 TECHNICAL REQUIREMENTS

4.1 The contractor shall accomplish the following on an order by order basis. The requirements for each order may encompass rapid Research & Development (R&D), trade space analysis and studies, design, prototyping, demonstration, scenario/concept development, experimentation and evaluation, integration, testing, technical installation, transition, and support through initial operations of technologies and solutions.

4.2 The following paragraphs identify the C-sUAS technical environments and focus areas to which specific orders may apply.

4.2.1 Information Exchanges and interfaces.

4.2.1.1 Evaluation of adapter/translator architecture that alleviates latency and complexity

4.2.1.2 Open architecture messaging as well as queueing and transformation services/middleware to evaluate messaging requirements such as guaranteed deliverability, durability, etc.

4.2.2 Electronic Warfare (EW) and Cyberspace Operations (CO.)

4.2.2.1 Seam between EW and CO.

4.2.2.1.1 Develop EW-enabled Cyberspace countermeasures (CM).

4.2.2.1.2 Develop CM to new sUAS C2 links as they emerge via techniques such as protocol manipulation, access denial, neutralization, spoofing, and operator deception.

4.2.2.1.3 Develop low collateral damage (CD) Electronic Attack (EA)/Cyberspace CM.

4.2.2.1.4 Improve RF/cyberspace contested environment performance and resiliency.

4.2.2.2 Defensive Cyberspace Operations (DCO) – develop advanced C-sUAS system DCO capabilities.

4.2.2.2.1 Cybersecurity hardening/resiliency by leveraging various AFRL and government off-the-shelf (GOTS) technology to improve resiliency of C-sUAS systems or its components.

4.2.2.2.2 Improve resiliency of friendly C-sUAS assets and technologies.

4.2.2.2.3 Prevent adversary access to friendly C-sUAS assets and technologies.

4.2.2.2.4 Preclude use of friendly nodes as pivot points for adversaries.

4.2.2.2.5 Apply anti-tamper technologies as needed to prevent loss or compromise of critical technologies.

4.2.2.2.6 Develop technologies and mechanisms to authenticate (i.e., positively identify) and track Blue Force Interceptors (BFI) and ensure that they have not been hijacked/coopted by the adversary.

4.2.2.3 Offensive Cyberspace Operations (OCO).

4.2.2.3.1 Develop technologies and techniques that provide immediate and near-real time Battle Damage Assessment (BDA) and cyberspace Situational Awareness (SA) of C-sUAS effects.

4.2.2.3.2 Develop “left-of-launch” capabilities – Note: further details omitted due to sensitivity.

4.2.2.4 Cyberspace C2.

4.2.2.4.1 Develop cyberspace CM and cyberspace C2, including R&D of handoff to cyberspace C2 systems of cyberspace payloads delivered by C-sUAS assets.

4.2.2.4.2 Develop user interface (UI) methods to enable selection of Cyberspace CM parameters for various operators.

4.2.2.4.3 Coordination/de-confliction of cyberspace CM from potentially different operators, including operators from different agencies.

4.2.2.5 Cyberspace Intelligence, Surveillance, and Reconnaissance (ISR).

4.2.2.5.1 Improve threat detection, identification, and tracking.

4.2.2.5.2 Note: further details omitted due to sensitivity.

4.2.3 C-sUAS Command and Control (C2).

4.2.3.1 Automation/autonomy for C2.

4.2.3.1.1 Develop technologies and solutions integrated with selected joint/AF GOTS C-sUAS tactical C2 solution(s), adding acumen to the existing C2 code without negatively impacting the user interface (UI), performance, or capabilities.

4.2.3.1.2 Develop technologies and solutions that leverage human-machine teaming to alleviate C-sUAS operator burden; this includes simultaneously operating a variety of C-sUAS modalities against mass/swarm attacks in complex engagement environments and scenarios.

4.2.3.1.3 Mature technologies and develop components or prototypes that enable the C-sUAS C2 system to understand and enforce Rules of Engagement (ROE).

4.2.3.1.4 Mature technologies and develop components or prototypes that enable the C-sUAS C2 system devise a recommended and optimized course of action (COA) for engagements involving mass/swarm attacks in complex engagement environments and scenarios where the C-sUAS system includes a variety of C-sUAS sensor and effector modalities.

4.2.3.1.5 Mature technologies and develop components or prototypes that integrate advanced C2 logic/automation focusing on human-machine teaming technologies that will enable a single operator to effectively engage a mass/swarm attack in complex engagement environments and scenarios where the C-sUAS system includes a variety of C-sUAS sensor and effector modalities.

4.2.3.1.6 Mature technologies and develop components or prototypes that automatically configure system components (i.e., sensors and effectors) based on ROE to reduce maintainer/operator burden and enables autonomy portion to track resource management of subsystems/components, including in a swarm-on-swarm environment where human operators would be overwhelmed.

4.2.3.2 Multi-domain C2 (MDC2).

4.2.3.2.1 Integration with higher-level C2 systems and external C4ISR systems.

4.2.3.2.2 Sensor/effector scope – ensure C2 technologies such as command sets account for a broad range of modalities such as URE and Directed Energy (DE) weapons.

4.2.3.2.3 Cooperation and de-confliction among cyberspace effects and other domain effects (e.g., cyber exploit telling threat to land and RF jammer causing it to hover), particularly in the case of a sUAS swarm.

4.2.3.2.4 Develop technologies and techniques to present MD options/COA to the operator and their probabilities of defeat.

4.2.3.2.5 Develop mechanisms and technologies to accurately assess and fuse confidence levels of various sensors and effectors from different domains/modalities.

4.2.3.3 Airspace Coordination Measures (ACM)/Air Traffic Control (ATC).

4.2.3.3.1 Develop technologies and solutions that interface existing systems such as joint ACM or ATC systems.

4.2.3.3.2 Develop technologies and solutions that interface prospective systems such as NASA's UAS Traffic Management (UTM) system.

4.2.3.4 Blue Force Interceptors (BFI).

4.2.3.4.1 Research and develop low-cost BFI prototypes leveraging COTS technology where appropriate to be used in C-sUAS and counter-swarm operations.

4.2.3.4.2 Develop low Size, Weight, and Power, plus Cooling/Cost, (SWAP-C) BFI payload solutions that enable threat detection, identification, and tracking from BFI platforms.

4.2.3.4.3 Incorporate BFI C2 leveraging COTS sUAS Application Programming Interfaces (API) and standards.

4.2.3.4.4 Integrate EW/CO capabilities.

4.2.3.4.5 Autonomy of platform movement and decision making.

4.2.3.4.6 Incorporate BFI C2 into MDC2 solution.

4.2.3.4.7 Incorporate BFI autonomous capabilities into C2 node autonomy to ensure effective control and alleviate conflicting actions.

4.2.3.4.8 Mature enclosures (e.g., pod, hive) that enable BFIs to be deployed in austere environments and positioned to intercept incoming threats at the boundaries of the protected area.

4.2.3.5 Sensors.

4.2.3.5.1 Acoustic.

4.2.3.5.1.1 Improve threat detection, identification, and tracking exploitation algorithms, including outside audible range (ultrasonic and infrasonic).

4.2.3.5.1.2 Research acoustic/sonic defeat mechanisms.

4.2.3.5.2 Active Emitting Technologies (e.g. Radar and Light Detection and Ranging [LIDAR]).

4.2.3.5.2.1 Explore leveraging existing radars (e.g., weather, ATC) to detect, ID, and/or track sUAS, especially those that are C2-silent (signal silent).

4.2.3.5.2.2 Explore leveraging LIDAR technologies to improve low-light conditions and environments where other sensors are less effective.

4.2.3.5.2.3 Develop technologies and solutions that employ active emissions to detect and ID C-sUAS threats.

4.2.3.5.3 Others as identified.

4.2.3.5.4 Unintended Radiated Emissions (URE) – Develop technologies and techniques that leverage threat URE to enable detection and identification.

4.2.3.6 Signature and Effects Library.

4.2.3.6.1 Methods for storing Cyberspace Effects (i.e., "Cyber Bullets") and indexing their capabilities.

4.2.3.6.2 Reverse engineer waveforms.

4.2.3.6.3 Methods of storing waveforms in a multi-level security environment.

4.2.3.7 Other emerging threats requiring research areas as COTS sUAS technology and the asymmetric threat advances.

4.3 Research and Development (R&D)

4.3.1 Collect, document, and analyze new user requirements with the goal of completeness, consistency, cost efficiency, and achievability. Collect requirements from attendees at conferences, user site visits, AF/DoD/Intelligence Community (IC) documents and publications, deployment site surveys, etc. Translate User requirements into a set of technical requirements (conforming to agile development approaches) to dictate the overall system design. User and technical requirements shall be presented to the AFRL/PM for approval. The Government shall establish a priority order for further investigation. See paragraph 4.6.4 for more details.

4.3.2 Analyze alternatives (i.e., perform trade studies) to explore various technical approaches for satisfying the requirements that are suitable for the intended operational environments. See paragraph 4.6.5 for more details.

4.3.3 Research and develop new capabilities and functionalities for C-sUAS. Develop a plan for implementation/integration into new or existing baselines.

4.3.4 Integrate new Open Architecture (OA) developments into existing or new system baselines. Ensure new baseline support the platforms with latest hardware components.

4.3.5 Ensure backward compatibility with legacy hardware in the Hardware Compatibility List (HCL) or as directed by the Government.

4.3.6 Develop capabilities for new components of OA to support next generation hardware processors and/or to reduce required patch queues. Ensure new development maintains a high degree of openness and that design decisions favor open solutions and technologies over those that bring some sort of constraints or tight coupling that limit the openness.

4.3.7 Develop technical capabilities to support for varying platforms to be added to HCL. Propose detailed hardware specifications, deletions, and/or substitutions to the appropriate Configuration Control Board (CCB) for approval.

4.3.8 Research, develop, and integrate new capabilities and functionalities to further develop system components.

4.3.9 Research, develop, and integrate new capabilities to C-sUAS software baselines. Ensure new C-sUAS baselines maintain support for all platform and components on legacy C-sUAS HCL or as directed by the Government.

4.3.10 For each new feature/capability, create feature design documentation. The feature design document shall include:

- Statement of feature
- One or more technical approaches (as applicable), including design or implementation alternatives and their pros/cons
- Architecture diagram
- User Interface (UI) changes and diagrams
- Impact analysis
- Data communication standards
- 3rd party technology incurred
- Derived requirements

4.3.11 The C-sUAS release shall implement requirements as stipulated on an order-by-order basis. Create documentation as described in paragraph 4.13 to reflect approved new baseline.

4.3.12 Provide the capability to include new features developed into enhancement or sustainment releases, implement per COTR guidance.

4.3.13 Develop a technology demonstration using sound software and hardware engineering principles as described in paragraph 4.5.

4.4 Enhancements

4.4.1 Enhance, and integrate emerging technologies and/or Commercial off the Shelf (COTS) platforms to build upon existing C-sUAS designs. Enhancements shall conform to existing system features and provide backward compatibility.

4.4.2 Follow procedures for any baselines changes as prescribed in paragraph 4.13.

4.4.3 Enhance capabilities, features, components, and other technologies and integrate them into approved C-sUAS systems.

4.4.4 Ensure enhanced systems baselines maintain support for all platform and components on legacy system HCL or as directed by the Government.

4.4.5 Maintain or improve existing capabilities of the currently baselined systems. Specifically, it shall:

- Not require any earlier versions to be installed
- Support an upgrade to the new version from the most recent previous version
- Be interoperable with the currently fielded versions, as well as any additional versions developed and released during the performance of this contract.

4.4.6 C-sUAS system enhancement shall implement requirements as stipulated on an order-by-order basis.

4.4.7 Update feature design documents to reflect changes made from the enhancement.

4.4.8 Revise documentation as described in paragraph 4.13 to reflect approved baseline changes. Provide Version Description Document (VDD) specific to this baseline update to reflect all changes incorporated into the baseline. Provide release notes and validation procedures for each baseline release.

4.4.9 Develop a technology demonstration using sound engineering principles as described in paragraphs 4.5 and 4.6.

4.5 Software Development

4.5.1 Employ agile software development processes and industry best practices. Practices shall incorporate software requirement/user story reviews, design reviews, code verification and

testing, security review, and appropriate interim deliveries as deemed necessary by COTR in coordination with the System Engineering Lead.

4.5.2 Ensure appropriate security controls are included in the design and implementation for an operational system, rather than just a R&D artifact. See paragraphs 4.15 and 4.16.8.

4.5.3 Apply industry best practices for well documented source code. Software development methodology shall incorporate appropriate source code control (e.g., Git or Subversion) in addition to a bug tracking (e.g., Jira, Bugzilla, or Mantis) for Problem Reports (PR), Change Requests (CR), Defect Report (DR) tracking. These practices are required throughout all phases of development.

4.5.4 Perform periodic code reviews to make continuous improvements in existing code aligned with coding best practices and to improve robustness of code. Ensure user friendly error handling is present in all code delivered.

4.5.5 Turn over source control, bug tracking, and related data to the Government as prescribed by the configuration management approach. The artifacts shall be in a format mutually agreed to by the performers and the Government per the CDRL.

4.5.6 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.6 System Engineering (SE)

4.6.1 SE Processes

4.6.1.1 This section outlines the SE and software development procedures that apply for all development, prototyping, enhancement, and sustainment efforts, unless otherwise specified by the COTR in coordination with the SE Lead.

4.6.1.2 Maintain a robust—but properly tailored—SE methodology for analysis, configuration, design, development, integration, and testing of C-sUAS systems components or prototypes.

4.6.1.3 Employ disciplined SE processes including, but not limited to, requirements development and management; modeling and simulation; technical management and control; system/software design and architecture; integrated risk management; configuration management; documentation management; coding; and test, evaluation, verification, and validation practices throughout the period of performance of task orders using properly tailored Life Cycle Systems Engineering process and industry best practices.

4.6.1.4 Employ a development methodology that is grounded in sound development processes and detailed reviews, ensuring justified progression to the next system engineering phases. Generate initial mockups and prototypes for all Graphical User Interfaces (GUIs) and utilize an evolutionary approach to create working models of all Configuration Items (CI) mapping back to the Work Breakdown Structure (WBS) and identified requirements. Provide these prototypes to the Government on a periodic basis determined on a case-by-case basis. Release schedules depend on the task order and component(s) being developed.

4.6.1.5 Provide the Government access to the SE processes and artifacts to support monitoring and review by the AFRL PM, COTR, and SE Lead.

4.6.1.6 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.6.2 Technology Development Standards and Tenets.

4.6.2.1 Develop technologies and solutions that, if applicable, comply with applicable Global Information Grid (GIG) Technical Guidance Federation (GTG-F) Standards (located here: https://gtg.csd.disa.mil) (formerly DoD Information Technology Standards Registry [DISR]); identify applicable standards for each component.

4.6.2.2 Develop technologies and solutions that enable cross-platform interoperability and platform-independence.

4.6.2.3 Develop technologies and solutions that are extensible to support future technology insertion and adoption.

4.6.3 SE Tools

4.6.3.1 Ensure development tool selection includes cross-tool integration to facilitate a smooth, effective association of data across the tool suite (e.g., software code repository linked to configuration management tool, test management and test automation linked to software build process/tools and defect tracker).

4.6.3.2 Provide Government access to tool suite to allow Government personnel insight into the development process and progress.

4.6.4 Requirements Engineering and Design

4.6.4.1 The requirements process is expected to be iterative: defining a portion up front to provide a foundation for starting the agile process and then evolving the requirements set over

time through repeated stakeholder interaction since not all the requirements will be known before design and implementation begins.

4.6.4.2 Provide technical management of these processes through requirements engineering (i.e., elicitation, analysis, documentation, and management), gap analysis, Tradespace analysis, solution architecture analysis, specified technical reviews, cybersecurity evaluation, and test/demo readiness and test/demo results reviews.

4.6.4.3 Design and implement solutions that are fully traced to requirements (i.e., requirements allocation). Provide traceability to sources such as demands signals. Track metadata to document where requirements/user stories originated (i.e., which stakeholder) That is, provide bi-directional traceability.

4.6.4.4 Document requirements as agile User Stories (or their equivalent) with story details that capture the requirements and acceptance criteria. Maintain User Stories for the duration of the period of performance and turn them over as a design artifact at the end. The format shall be a mutually agreed format that is conducive to future development and operations and sustainment of the work products.

4.6.4.5 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.6.5 Decision Analysis

4.6.5.1 Document Tradespace analysis and design decisions with the appropriate level of rigor according to the risk involved. These may be informal notes by developers or engineers for less formal decisions or a Decision Analysis Report for more involved decisions.

4.6.5.2 Tradespace will be driven by requirements, Concept of Operations (CONOPS)/Concept of Employment (CONEMP), technology maturity, and related factors.

4.6.5.3 Establish and maintain guidelines to determine which issues are subject to a formal evaluation process. Maintain guidelines for documenting decision analysis for each level of rigor and ensure they are consistently applied by developers.

4.6.5.4 Determine technical review requirements and associated entry/exit criteria.

4.6.5.5 Identify, document and evaluate alternative solutions to program requirements.

4.6.5.6 Identify and down-select appropriate criteria for each trade study. Include aspects such as benefits to stakeholders, particularly end users, including, but not limited to, improved functionality, cost efficiency, scalability, reducing operator burden, increasing system suitability

and effectiveness, etc. Consider constraints and risks with respect to technical, cost, and schedule.

4.6.5.7 Required Artifacts.

4.6.5.7.1 Decision guidelines, including evaluation criteria and methods.

4.6.5.7.2 Technical review entry/exit criteria and meeting minutes.

4.6.5.7.3 Trade studies/tradeoff analyses.

4.6.5.7.4 Decision briefings or formal reports (as applicable).

4.6.5.8 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.6.6 Technical Reviews

4.6.6.1 Include appropriate technical reviews based on the work products associated with the task order. Appropriate technical reviews may include:

- System Requirements Review (SSR)
- System Functional Review (SFR)
- Software Specification Review (SSR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)
- Government Acceptance Test (GAT)
- Factory Acceptance Test (FAT)
- System Verification Review (SVR)
- Operational Readiness Review (ORR)

4.6.6.2 Prepare presentation materials, documentation, and artifacts in advance of the reviews and submit per the CDRL.

4.7 Hardware/Software Procurement

4.7.1 Procure and deliver commercial software and hardware necessary for system integration and troubleshooting to include COTS software licenses as approved by the government.

4.7.2 Coordinate any hardware procurement with the AFRL PM, SE Lead, and COTR to ensure that all steps necessary for shipment, delivery, and acceptance of any purchased equipment has been identified and accomplished.

4.7.3 GFE will be specified in each task order. Procure additional hardware as Contractor Acquired Property (CAP) in consultation with the COTR.

4.7.4 Prepare documentation and artifacts per the CDRL.

4.8 Integration

4.8.1 Identify required interfaces, both human and machine, during the requirements and design phases. Validate the Interface Control Document (ICD) versions and applicable standards for every legacy or new external interface. List all industry or military standards for each interface.

4.8.2 Identify internal interfaces and describe and document all applicable military or industry standards to which the interface must/will conform.

4.8.3 Identify all Human-Machine Interfaces (HMI), also known as User Interfaces (UI) in many cases, pertaining to the system, component, or prototype. Describe and document all applicable military or industry standards to which the interface must/will conform. Provide mockups of all HMI/UI in advance of implementation and garner stakeholder input to the design. This includes modifications to existing HMI/UI.

4.8.4 Integrate development components with legacy or new components.

4.8.5 Perform the necessary integration testing per paragraph 4.9.

4.8.6 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.9 Testing

4.9.1 Perform thorough Verification and Validation (V&V) for each release/enhancement/baseline to ensure compliance with functional, non-functional, and security requirements.

4.9.2 Research, Development, Test, and Evaluation (RDT&E)/Developmental Test and Evaluation (DT&E) -- For each operational release, enhancement, or new baseline development, perform thorough, multi-faceted testing as appropriate from the list below:

- Unit testing
- Integration testing
- System testing
- Regression testing
- Cybersecurity (security/Security Technical Implementation Guides (STIG)/NIST conformance) testing
- Backlog bug fix V&V
- Performance testing (stress (load)/longevity term)

- Component configuration validation
- Hardware environmental testing

4.9.3 Employ various testing approaches and best practices as applicable such as fuzzing, symbolic execution, and equivalence partitioning to fully explore internal and external interfaces and system/component stability and resiliency.

4.9.4 Employ equivalence partitioning and other techniques to ensure system or component properly handles both valid and invalid inputs and gracefully recovers from fault conditions and handles all foreseen error conditions and performs exception handling.

4.9.5 Automate unit, integration, system, and regression testing as much as feasible given the nature of the development environment and budget. Apply agile software development methods such as continuous integration and continuous testing.

4.9.6 Apply open systems tenets using proven but modern languages, tools, and design patterns.

4.9.7 Create stubs as needed to complete necessary testing. Identify GFI at least sixty (60) days in advance that are needed for testing.

4.9.8 Ensure each test case is mapped to requirements and correspondingly mapped to test cases/test procedures. Provide transparency of test execution, status, and results by maintaining a complete and robust test management process.

4.9.9 Create test report(s) to include test cases executed, expected test results, actual test results, issues encountered, test duration, and metrics (where they can be leveraged to gain efficiencies and insight to improve the process).

4.9.10 Prepare materials for and support Test Readiness Reviews (TRR) when major test event or demos are planned. Gain consensus with Government stakeholders on TRR entrance and exit criteria.

4.9.11 Update all applicable design, test, security, and training documentation to reflect results, issues, and mitigation of testing.

4.9.12 Identify special test equipment (STE), facilities/ranges, resources, GFE, and GFI as early as possible to allow for proper coordination among stakeholders and reservation.

4.9.13 Flight Testing

4.9.13.1 The Government is responsible for management of the Flight Test Plan (FLP). The performer shall support preparation of the FTP by providing detailed data as required by the COTR.

4.9.13.2 Provide presentation materials and other documentation needed to support the Technical Review Board (TRB).

4.9.13.3 Attend boards applicable to the individual order with expertise covering all aspects of the testing such as electromagnetic radiation, platform or payload performance, data gathering requirements, and test resources such as STE.

4.9.14 Support Operational Test and Evaluation (OT&E) events as approved by the COTR and/or as prescribed in theindividual order.

4.9.15 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.10 Hardware/Software Delivery

4.10.1 Deliver all software and hardware developed, assembled, or acquired to the Government in accordance with the Order schedule and the following:

4.10.1.1 Deliver a copy of all software developed under this effort as source and object (executable) code. Include the commented source listings and source code.

4.10.1.2 Design the software to make use of existing software and for subsequent reuse to the maximum extent possible where technically and fiscally sound.

4.10.1.3 Developed software under this effort is to be completely maintainable and modifiable with no reliance on any non-delivered computer programs or documentation.

4.10.1.4 Deliver the baseline changes made in support of the new version/patches as source code on CD-ROM or DVD. This CD/DVD shall contain enough information for the Government COTR to recreate the build environment including, but not limited to the compiler, Operating System (OS), OS patches, all run-time libraries, middleware, compile or build files, and test code (i.e., stubs and scaffolding). Digital deliveries may be utilized per Government guidance. Commercial tools for which the Government does not own a license need not be included. Source code shall not be delivered to any other organizations without written permission of the COTR. Forward requests for source code releases to the COTR.

4.10.1.5 Deliver systems with clearly defined version numbers (both hardware and software) per paragraph 4.13.

4.10.1.6 Per software delivery, deliver instructions for complete recreation of the build environment. Provide any custom tools and build scripts used to create the build environment that are not readily available or open source.

4.10.2 Acquire Government approved hardware incidental to the design and development, to support system requirements, development or demonstration of prototypes, or system development (testing, prototyping) activities. Include licensing, maintenance, and diagnostics support software and STE. Arrange for delivery of hardware, software, and licenses to Government designated sites.

4.10.3 Prepare documentation and artifacts per the CDRL.

4.11 Deployment

4.11.1 System Delivery and Deployment

4.11.1.1 Complete all new deployments in accordance with process described below.

4.11.1.2 Complete all enhancements in accordance with process described in paragraph 4.4.

4.11.2 Procure hardware (per paragraph 4.7) for customer sites and perform system deployments at designated sites.

4.11.3 Perform system deployments and installations at site facilities applicable to the task order. Perform upgrades to systems operational sites.

4.11.4 Provide the capability to support simultaneous deployment installations at any given time.

4.11.5 Deployment Process

4.11.5.1 Conduct Site Survey

4.11.5.1.1 Perform location selection, Line of Site (LOS) analysis, RF survey, and collect other relevant information for the installation.

4.11.5.1.2 Provide an Installation Plan that includes the results of the site survey will be used to finalize the implementation approach for the site to include project schedule, conceptual site architecture, hardware and software recommendations, and detailed description of the system

configurations. The proposed installation shall facilitate the smallest impact possible to each site upon deployment of equipment.

4.11.5.2 Site Preparation

4.11.5.2.1 Plan the incorporation of the system into the individual site. Assist site with development of site specific CONOPS or CONEMP.

4.11.5.2.2 Provide site with guidance on creating and submitting required security documentation such as Standard Operating Procedures and System Security Plan.

4.11.5.2.3 Schedule site installation in coordination with site stakeholders and deconflict with other order activities.

4.11.5.2.4 In advance of actual install, conduct a Site Readiness Review (SRR) via teleconference to ensure all equipment, personnel, and approvals are finalized and ready for installation.

4.11.5.3 Installation

4.11.5.3.1 Ensure familiarization documentation is completed per paragraph 4.11.6 before deployment.

4.11.5.3.2 Perform site installs per the order and developed Installation Plan.

4.11.5.4 Post-Installation Support

4.11.5.4.1 Provide engineering support for system familiarization as specified in paragraph 4.11.5.5.

4.11.5.4.2 Coordinate and conduct site installation and integration with site personnel.

4.11.5.4.3 Provide post installation quick reaction support to mitigate issues not discovered during installation.

4.11.5.5 Prepare documentation and artifacts per the CDRL.

4.11.5.6 Familiarization Design and update familiarization curriculum to reflect baseline modifications.

4.11.5.7 Develop familiarization material for different classes of personnel associated with the system (e.g., installers, operators, administrators, and maintainers), to include train-the-trainer materials, as prescribed by the order.

4.11.5.7.1 Develop familiarization materials and conduct training for integrator/installers, including requisite knowledge required to install, configure, and check-out the system.

4.11.5.7.2 Develop familiarization materials and conduct sessions for operators (end users).

4.11.5.7.3 Develop familiarization materials and conduct sessions for tier one (1) and two (2) help desk personnel.

4.11.5.7.4 Develop familiarization materials and conduct sessions for system administrator, Field Service Engineer (FSE)/Field Service Representative (FSR), and maintainer course, including requisite knowledge required to configure, administer, and troubleshoot the system.

4.11.5.8 Curriculum shall consist of classroom lecture presentations and significant hands-on exercises. Operator familiarization will include various, realistic engagement scenarios that exercise the full capabilities of the system. This familiarization will include significant time on the actual system or a realistic, accurate simulator.

4.11.5.9 Provide familiarization equipment as prescribed by the order.

4.11.5.10 Develop and update admin and user guides to reflect baseline changes, include lessons learned during testing, allow for troubleshooting, and improve accessibility for novice users.

4.11.5.11 Prepare documentation and artifacts per the CDRL.

4.12 Sustainment

4.12.1 Devise and document a maintenance concept that is compatible with existing baseline sustainment for all new components, prototypes, systems, or system updates.

4.12.2 Provide system maintenance, testing, help desk, and quick reaction support for all operational/deployed versions of systems, including any additional versions developed and released during the performance of the contract. Integrate and test security and operating system patches. Identify, in detail, the required patches in the Installation and Configuration Guides (ICG).

4.12.3 Develop, test, document, and deliver copy of CCB approved software/hardware changes per paragraph 4.13.

4.12.4 Satisfy applicable testing requirements per paragraph 4.9.

4.12.5 Quick Reaction Support and Time-sensitive Changes

4.12.5.1 Respond to system problems of a critical nature as specified in the order, IAW the CCB charter and CCB work flow per paragraph 4.13. This includes, but is not limited to, analyzing the problem and develop, test, document, and implement the solution for the site(s).

The fix shall contain release notes, validation procedures, installation instructions, removal (backout/rollback) procedures, and be operationally compatible with the supported version(s). Use software/hardware maintenance techniques, configuration management procedures, and methods to maintain close coordination with Government.

4.12.5.2 Provide the Government a work plan in a timeline proportional to the problem severity.

4.12.5.3 Incorporate all Quick Reaction fixes into the next scheduled release of the baseline unless directed otherwise by the cognizant CCB.

4.12.5.4 If called for by the maintenance concept, provide a maintenance capability for the existing baseline software.

4.12.6 Periodic Releases

4.12.6.1 Provide periodic sustainment releases to operational baselines approximately every quarter to incorporate CCB-approved baseline changes.

4.12.6.2 Support CCB decisions to determine appropriate content in each formal release.

4.12.6.3 Revise documentation as described in paragraphs 4.18 and 4.13 to reflect approved baseline changes.

4.12.6.4 Evaluate changes incorporated into each baseline release and identify appropriate functional and security testing. Test each baseline release for compliance with functional and security requirements IAW paragraph 4.9. Ensure updates to each major baseline maintain support for legacy platforms included in Hardware Compatibility List (HCL). Report developer test results and readiness at TRR.

4.12.7 Help Desk

4.12.7.1 Provide Tier 1 and Tier 2 support via help desk, on-call support as specified in the task order. Support all deployed versions of software, documentation, and site infrastructure configurations at all deployment sites.

4.12.7.2 Utilize an automated Help Desk Tracking System to maintain and track each call to the Help Desk. Provide metrics regarding help desk activity, problem types, resolutions, etc. Document all Help Desk problems and their status within the AFRL Program Management Reports.

4.12.7.3 Consolidate help desk tickets at least weekly to maintain synchronicity.

4.12.7.4 Integrate ticketing system findings with bug tracking and change request systems/tools.

4.12.8 Tier 3 Engineering Support

4.12.8.1 Provide Tier 3 support using Subject Matter Experts (SME) on the system components on-call support as specified in the task order.

4.12.8.2 Tier 3 support shall include all the appropriate engineering disciplines: systems, software, mechanical, electrical, RF, etc. as appropriate for a given system.

4.12.9 Onsite Support

4.12.9.1 Provide onsite engineers at deployed sites as specified in the order (i.e., FSR or FSE) as to provide expertise and assist sites in transitions and ongoing operational support until such time military personnel or a future support contract subsumes this function.

4.12.9.2 Provide onsite FSE/FSR at sites determined by the COTR.

4.12.9.2.1 For each site, provide system integration, deployment, and sustainment activities within the customer site enterprise.

4.12.9.2.2 Assist site staff to resolve administration and management issues.

4.12.9.2.3 For each site, provide familiarization activities at customer site.

4.12.9.2.4 For each site, provide engineering, integration, and testing of the of the C-sUAS system to include Small UAS Operator (SUASO)-qualified FSEs, if required in the task order, for operational system checks and range/performance testing.

4.13 Configuration Management (CfM)

4.13.1 Apply applicable CfM process and procedures such as those prescribed by Information Technology Infrastructure Library (ITIL) or Capability Maturity Model Integration (CMMI).

4.13.2 Ensure all baseline changes are tracked and reproducible from inception to completion.

4.13.3 Participate in Configuration Control Board (CCB) meetings and processes. Abide by CCB decisions and submit pending changes to the CCB before taking action on them.

4.13.4 Notify AFRL PM, SE Lead, and COTR of any unapproved changes to baselines. Any changes, however small, must be acknowledged and approved by the AFRL PM and/or technical lead. Ensure all design, test, security, user, and training documentations are updated accordingly.

4.13.5 All system documentation created by the contractor shall be maintained on a configuration control system for version control and traceability. The CM system shall be accessible by Government personnel for review and synchronization between the government and the contractor. Two-factor authentication shall be used to ensure data security.

4.13.6 Provide Software Version Document (SVD) specific to each baseline update to reflect all changes incorporated into that baseline. Provide release notes and validation procedures for each baseline release.

4.13.7 Devise a versioning scheme and assign version numbers for hardware and software and apply serial numbers to hardware in consultation with the COTR under the advice of the applicable CCB.

4.13.8 At appropriate milestones, conduct a Functional Configuration Audit (FCA) to ensure the work product(s) meet requirements and quality assurance factors and a Physical Configuration Audit (PCA) to ensure the technical data package matches the work product(s).

4.13.9 Ensure CfM approach is compatible with agile software development methods and tools.

4.13.10 Provide Software Version Document (SVD) specific to new baseline to reflect all changes incorporated into the baseline. Provide release notes, validation procedures, and training material for each baseline release.

4.13.11 Change Requests (CRs)

4.13.11.1 CRs may come in the form of enhancement requests or Problem Reports (PR), aka bugs or Discrepancy Reports (DR).

4.13.11.2 Present CRs during the C-sUAS CCB, bolstered with impact analysis, design alternatives, etc. Provide a subject matter expert to discuss the PRs at each CCB.

4.13.11.3 Support CCB decisions with estimates for completing changes such as associated labor hours, task dependencies, accreditation issues, affected system components/CSCs, estimates for updates to the documentation, etc. Provide a scope of impact analysis of the recommended change(s), including determination whether any of the testing cycles have to be repeated (i.e., regression testing) due to the modifications made to the baseline.

4.13.11.4 Create work plans for CCB approved CRs. Submit work plans for CRs in accordance with the C-sUAS CCB Process. Identify the work to be accomplished with AFRL PM approval

and guidance, a recommended solution, required resources, accreditation issues, and estimates for updates to the documentation. Provide a scope of impact analysis of the recommended change(s).

4.13.11.5 Develop, test, document, and deliver software versions to resolve CCB approved CRs. Upon CR work plan approval by Government, proceed with the development, integration, testing, and documentation. Provide release notes, validation procedures, installation instructions, and removal (i.e., backout/rollback procedures) instructions for all CRs.

4.13.12 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.14 Quality Control (QC)

4.14.1 Employ and maintain a quality program to ensure development efforts are in accordance with commonly accepted industry best practices. These processes shall be used throughout this contract lifecycle and ensure high-quality analysis, design, development (including use of prototyping and modeling & simulation), coding, integration, testing, training, demonstration, documentation, schedule, delivery, deployment, maintenance, and support as they pertain to the task order.

4.14.2 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.15 Program Management (PM)

4.15.1 Determine the status of each task order and report progress towards accomplishment of the requirements at the period prescribed by the CDRL. Based on an order by order basis, reporting may be required to be distributed to the AFRL PM and the designated COTR.

4.15.2 Determine the status of funding required for order performance at the period prescribed by the CDRL. Based on an order by order basis, reporting may be required to be distributed to the AFRL PM and the designated COTR.

4.15.3 Conduct oral presentations at such times and places designated in the task order schedule. Provide status of technical progress made to date in performance of the task order during presentations. Based on an order by order basis, reporting may be required to be distributed to the AFRL PM and the designated COTR.

4.15.4 Risk Management

4.15.4.1 Actively and continuously identify and manage technical, cost, and schedule risks. Keep the AFRL PM and designated COTR informed of risk status and handling plans on a monthly basis or sooner if warranted by the risk level or related events. Immediately inform the AFRL PM if any risk is realized and becomes an issue.

4.15.4.2 Identify, assess, and track issues in addition to risks. Keep the AFRL PM and designated COTR informed of issue status and recovery plans on a monthly basis or sooner if warranted by the consequences or related events.

4.15.4.3 Identify, assess, and track opportunities in addition to risks. Keep the AFRL PM and designated COTR informed of opportunities on a monthly basis or sooner if warranted by the potential benefits or related events. Clearly articulate and assess any risks associated with pursuing any opportunity.

4.15.4.4 Apply industry best practices for risk, opportunity, and issue identification, assessment, and handling.

4.15.4.5 Ensure risks are not accounted for at multiple levels thereby overcompensating for them (e.g., engineer provides engineering margin to account for the risk, then the PM applies additional margin accounting for the same risk). This applies to basis of estimates for risk level, time, cost, etc.

4.15.5 Integrated Master Schedule (IMS)

4.15.5.1 Create, update, and maintain an IMS. The schedule shall include Original Start and Original End dates, which will not be changed after task award; Baseline Start and Baseline End dates, which reflect the current task baseline and shall not be changed without Government concurrence; and Actual Start and Actual End dates, which represent the actual dates the activities will or did occur.

4.15.5.2 Provide a detailed breakdown of all required reviews that demonstrate keen insight into the software development process. Provide projected start and completion dates for all tasks, including projected dates for all evolutionary software prototypes to be delivered to the Government. At a minimum, the IMS milestones shall include the appropriate technical reviews, final code delivery, and document delivery dates.

4.15.5.3 Provide status of all baseline development, test, training, schedule, and sustainment activities at the regularly scheduled C-sUAS Integrated Product Team (IPT) meetings and when directed by the COTR.

4.15.6 Document all technical work accomplished and information gained during performance of each task order. Include all pertinent observations, nature of problems, positive and negative results, and design criteria established where applicable. Document procedures followed, processes developed, "Lessons Learned," etc. Document the details of all technical work to permit full understanding of the techniques and procedures used in the evolving technology or processes developed. Cross-reference separate design, engineering, or process specifications delivered to permit a full understanding of the total acquisition.

4.15.7 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.16 Security Requirements

4.16.1 Manage all aspects of security associated with performance to include personnel security access, security clearance information preparation, and liaison with Government POCs for security related items. Capture and maintain information regarding all contract personnel and security related data. The personnel information maintained and provided to the AFRL PM shall include a list of all personnel performing under the contract, security clearance levels, sponsors, dates for performance, and government identification materials (i.e. Common Access Cards (CACs), agency badges). Provide information supporting visit requests, CACs, personnel clearance, and other security related activities. Provide softcopy and hardcopy of managed information assuring proper privacy markings and controls are utilized. Format will be Contractor-suggested, Government-approved format.

4.16.2 Access To Private Information: Performance may require access to information covered by the Privacy Act of 1974; therefore, contractor personnel shall safeguard all such information in accordance with the Privacy Act of 1974 at all times, and shall not release such information to unauthorized persons.

4.16.3 Export Control: The Contractor may be required to carry out technical data/information exports in support of the requirements. Ensure all items have appropriate control markings to include Scientific and Technical Information (STINFO), export control and classification. Comply with applicable International Traffic in Arms Regulations (ITAR) requirements to meet the needs of the Government. Maintain compliance with all governing directives and policies. Prepare and submit required Export Control documentation and requests with the appropriate Government department or agency.

4.16.4 Security Clearance: Compliance with DoD 5200.2-R, Personnel Security Program, January 1987 for access to Top Secret/Special Compartmented Information (TS/SCI) information, systems and facilities is mandatory. All contractor personnel shall be citizens of the United States of America.

4.16.5 Safeguarding Classified Information

4.16.5.1 Comply with the DD Form 254, *DoD Contract Security Classification Specification* and attachments. Potential security violations or incidents shall be reported immediately to the AFRL PM and in writing no later than the next work day after the incident occurred. Proper controls shall be utilized (i.e., secure telephone, classified fax, classified e-mail), based on the security classification of the information associated with the possible violation.

4.16.5.2 Conform to the provisions of DoD 5220.22-M, *National Industrial Security Program Operating Manual* (NISPOM), for safeguarding classified information and material contained on the controlled system(s)/network(s). Ensure access is provided only to those persons who have the proper security clearance, a need to know and have been trained in proper safeguarding procedures.

4.16.5.3 Participate in the management of security access, preparation of security clearance data/forms, access requests, and coordination with Government security POCs.

4.16.6 Physical Security

4.16.6.1 Comply with the requirements as specified on an order by order basis and individual base support letters.

4.16.6.2 Safeguard all Government property. Ensure all Government facilities, equipment, and materials are secured. Follow regulatory guidance concerning maintenance, use, and safety of Government facilities.

4.16.6.3 For performance of services during emergency conditions, local procedures shall be followed.

4.16.7 Security Violations - Potential security violations or incidents shall be reported immediately to the Government PM verbally and in writing no later than the next work day after the incident occurred or was discovered.

4.16.8 Cybersecurity/Information Protection (IP)

4.16.8.1 Provide cybersecurity/Information Protection (IP) support IAW the Government's cybersecurity policies, standards/regulations, and requirements/planning, as referenced in the system Security Control Traceability Matrix (SCTM) and National Institute of Standards and Technology (NIST) 800-53. Cybersecurity/IP support shall include vulnerability assessments, remediation, and mitigation that are compliant with the most current AF, Defense Information Systems Agency (DISA), and DoD regulations and guidance.

4.16.8.2 Provide a system to meet the requirements for a DoD Risk Management Framework (RMF), IAW the listed documents or their most current versions, as applicable:

- NIST SP800-37 Rev 2, *Guide for Applying the Risk Management Framework to Federal Information Systems*
- NIST SP800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- AFMAN 17-1303 – *Cybersecurity Workforce Improvement Program*
- AFMAN 17-1301 – COMPUSEC
- AFI 17-101 – *Risk Management Framework for AF IT*
- AFI 17-130 – *AF Cybersecurity Program Management*
- AFI 33-360 – *Publications and Forms Management*
- AFMAN 33-363 – *Management of Records*
- AFPD 17-1 – *Information Dominance and Cyberspace Governance and Management*
- CNSSI No. 4005 – (FOUO) *Safeguarding Communications Security (COMSEC) Facilities and Materials*
- CNSSI No. 4016 – (FOUO) *National Information Assurance Standards for Risk Analyst and the Risk Management*
- DoDI 8500.01 – *Cybersecurity*
- DoDI 8420.01 – *Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies*
- DoDI 8520.02 – *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*
- DoDI 8540.01 – *Cross Domain (CD) Policy*
- DoDI 8520.03 – *Identity Authentication for Information Systems*
- DoDI 8551.01 – *Ports, Protocols, and Services Management (PPSM)*
- DoDI 8580.1 – *Information Assurance (IA) in the Defense Acquisition System*
- DoDD 8570.01 – *Information Assurance Training, Certification, and Workforce Management*
- DoD 8570.01-M – *Information Assurance Workforce Improvement Program*
- CJCSI 6510.01F – *Information Assurance (IA and Computer Network Defense (CND)*
- DoDI 8510.01 – *Risk Management Framework (RMF) for DoD Information Technology (IT)*

4.16.8.3 Ensure all new, enhanced, and sustained baselines satisfies applicable NIST 800-53 security controls as documented in system SCTM.

4.16.8.4 Support application of DISA Security Technical Implementation Guides (STIGs) against all system development, enhancement, and sustainment efforts and all applicable development, testing, and deployed environments. Support shall include:

- Identify applicable STIG for each component, prototype, or system
- Running STIGs through scanning capabilities or manual checks.
- Documenting STIG test scripts, expected outcomes, and test results.
- Delivering STIG results to Government PMO
- Reviewing STIG findings.
- Developing remediation steps and schedules (i.e., Plan of Action and Milestones (POA&M)).
- Identifying impacts of remediation approaches to DEAMS operations.
- Revising designs to accommodate or implement remediation.
- Performing Government review of solution designs.
- Developing workarounds to mitigate identified vulnerabilities.

4.16.8.5 Conduct automated source code analysis (SCA) on every release/patch that includes new or modified source code. Deliver an SCA Report for each release/patch/baseline that includes new or modified source code.

4.16.8.6 Report suspected vulnerabilities and security incidents in accordance with AFI 33-138, 5 Nov, Enterprise Network Ops Notification and Tracking. Respond to Air Force Computer Emergency Response Team (AFCERT) advisories in accordance with AFI 33-138 as follows:

4.16.8.6.1 Acknowledge receipt of AFCERT advisories within seven (7) days of issue. Evaluate each advisory for applicability and impact to system baseline.

4.16.8.6.2 Monitor additional sources of advisories for potential applicability to system to include the following:

- http://www.cert.org/vulnerability-analysis/knowledgebase/index.cfm
- https://nvd.nist.gov/
- https://access.redhat.com/security/security-updates/#/
- http://securitytracker.com/archives/summary/9000.html
- https://www.us-cert.gov/
- http://cve.mitre.org/cve/
- http://seclists.org

4.16.8.6.3 Implement the countermeasures identified by the advisory within the timeframe specified by the advisory or as specified by the Government COTR. If the countermeasures cannot be implemented, document the inability and obtain approval from the Designated Accrediting Authority (AFI33-200 23 Dec 08, IA Management) and the Government either for

an alternative corrective action or to continue operations without the countermeasures. If alternative corrective action is approved, implement this action within the timeframe specified by the Government.

4.16.8.6.4 Acknowledge receipt of and be prepared to implement countermeasures to include, but not limited to the following advisories: CERT (http://www.cert.org), DOD-CERT, JTF-GNO IAVA, Debian, StrongSwan, Cisco/AnyConnect, Citrix Receiver for Linux, VMware Horizon View client, RDP client, Open SSL, RHEL errata, NIST CVE, Xen Security Advisories, OpenEmbedded, and QEMU that affect the system baseline as directed by the Government.

4.16.8.7 Test the latest patches on each supported operational system at least once to verify compatibility with the latest fielded release.

4.16.8.8 Per deployment, provide Security Assessment and Authorization (A&A) support to sites in support of system installations. A&A support include, but are not limited to, helping sites define their System Security Authorization Agreement (SSAA), prepare Standard Operating Procedures (SOPs) and offering guidance on how to obtain Top Secret and Below Interoperability (TSABI) and/or Secret and Below Interoperability (SABI) tickets and Interim Authority to Test (IATT) with the goal of the site obtaining a permanent Authority to Operate (ATO). A&A support will be required throughout system site surveys, installation, and A&A process.

4.16.8.9 Monitor changes/updates/alerts in security controls, STIGs, OpenXT communities, and Cross Domain communities. Notify AFRL PM of any issues. Remediate per AFRL PM direction.

4.16.8.10 Provide personnel that meet DoDD 8140 and 8570 Baseline Certification requirements. Provide personnel possessing IAM Level II certification and IAT level III certification. Provide personnel with at least 10 years of experience in cybersecurity fields. Provide personnel with experience in RMF, TSABI, and SABI accreditation.

4.16.8.11 Provide engineering input to the AFRL PM with security assessments. At the Government’s request, provide Subject Matter Experts (SMEs) to collaborate with security assessors at assessment locations.

4.16.8.12 Ensure security documentations are updated with latest security information and consistent with latest policy and guidance.

4.16.9 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.17 Safety Requirements

4.17.1 Comply with all safety and health requirements necessary for the protection of personnel, facilities and equipment including, but not limited to, the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and all applicable OSHA standards, while performing this contract at the Air Force Research Laboratory (AFRL), Rome Research Site (RRS), Rome NY. It is the contractor's sole responsibility to make certain that all safety requirements are met.

4.17.2 Maintain a written safety program for compliance with the applicable OSHA standards, and make said program available for review by the Government upon request by the Contracting Officer.

4.17.3 Support Government Safety Review Board (SRB) and related activities, by preparing necessary documentation or briefings. Provide detailed data to support establishment adequacy or conformance such as test platform and payload airworthiness. See section 4.9 for TRB and flight test plan information.

4.17.4 In the event of a mishap, or a "near miss" during the performance of this contract at AFRL RRS, notify the Contracting Officer, COTR, or the DET 4 Safety Office no later than the next business day. Written notification shall be provided to the Contracting Officer (who will forward a copy to the DET 4 Safety Office) within 72 hours and shall include the following information (Air Force Form 978 Supervisors Mishap Report may be used):

- Contract, Contract number, Name and Title of Person(s) Reporting
- Date, Time and exact location of accident/incident
- Brief Narrative of accident/incident (events leading to accident/incident)
- Cause of accident/incident (if known)
- Type of injuries resulting from the accident/incident and estimated cost of accident/incident (material and labor to replace/repair)
- Nomenclature of equipment involved in accident/incident
- Personnel involved in accident/incident
- Corrective Actions (taken or proposed)
- Other pertinent information

4.17.5 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.18 Reports and Documentation

4.18.1 Notify the government at least weekly of source code changes, bug reports, and known

issues.

4.18.2 Deliver new and revised documents for the models, components, prototypes, or systems. Ensure new and revised documents meet or exceed the requirements, quality, style, and format of the existing documentation. See CDRL for a list of system documentation to be created or revised with a set of updates required for each release except where noted.

4.18.3 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.19 Travel

4.19.1 Participate in technical assistance visits, integration visits, site surveys, Technical Exchange Meetings (TEM), testing events, demonstrations, and program or technical reviews as required by the task order.

4.19.2 Coordinate specific travel arrangements with the individual COTR or AFRL PM to obtain advance, written approval for the travel about to be conducted. The contractor's request for travel shall be in writing and contain the dates, locations, and estimated costs of the travel.

4.19.3 Prepare necessary visit requests and coordination needed to attend a given meeting or event (with the advanced notice prescribed by the location/site).

4.19.4 Overseas travel: Comply with all government foreign travel requirements as specified by each task order. Additional information and/or training maybe required on a country by country basis.

4.19.5 Unless otherwise specified by the Government, develop a Trip Report detailing, at a minimum, stakeholder positions/feedback, accomplished tasks, unaccomplished tasks, open issues, and new issues.

4.19.6 Prepare presentation materials, documentation, and artifacts per the CDRL.

4.19.7 Meeting Attendance

4.19.7.1 Attend prescribed meetings such as Technical Exchange Meetings (TEMs), technical reviews, and conferences.

4.19.7.2 Meeting attendance will be a combination of teleconferences, video conferences, and in-person, depending on the task order.

4.19.7.3 Attend and document meetings/working groups with Government executives, System Managers, and others within various Government agencies. Maintain the minutes of these

meetings and distribute to Government personnel to gain consensus of their accuracy. Review all materials provided at the meetings/working groups to determine engineering and integration issues.

4.19.7.4 Document all trips to sites, agencies, conferences, or other organizations detailing the following: purpose, location, attendees, summary of discussions/events, issues, Tradespace, decisions, action items, and any other pertinent information.

4.19.7.5 Provide conference and presentation capabilities, as approved by the Government, to allow for the presentation of prototypes, technical program information, and issues. Address all aspects of coordinating, acquiring (e.g., booths, supplies, shipping, multi-media, displays etc.) and configuring space to perform the required demonstration and/or presentation. Activities may include professional development seminars, demonstrations, trade shows, conferences, and briefings relating to integration issues or programs as identified by the COTR.

4.19.7.6 Prepare presentation materials, documentation, and artifacts per the CDRL.