Joint Cyber Command and Control (JCC2)
Field Application Engineering
Statement of Work (SOW
25 July 2024

Name:	JCC2 Field Application Engineering
Organization:	Cryptologic and Cyber Systems Division (AFLCMC/HNCJ)
Address:	230 Hall Blvd, San Antonio, TX 78226

Table of Contents

1. PURPOSE

The objective of this JCC2 program is to provide the DoD, through Air Force Life Cycle Management HNC (AFLCMC/HNC), technical and expert level support to the Joint Staff, Combatant Commands and the Services. This effort will provide the Joint Force with JCC2 Training and Field Application Engineering to integrate and optimize the range of current and future JCC2 applications across the Department of Defense (DoD).

2. Background

The JCC2 program consists of, Battle Management, Threat Awareness Sharing Capability (TASC), and Mission Assurance Decision Support System (MADSS) applications and have achieved remarkable success over the course of the programs by developing, delivering and sustaining enterprise level platforms and capabilities that successfully integrates global operations in support of cyber operations by the Joint Force. This success was powered through the combination of stakeholder engagement and support, coupled with the ability to rapidly prototype and deliver capabilities. The transition from a prototype managed by the Strategic Capabilities Office (SCO) to an Air Force managed program has enabled the next step in the evolutionary process that will see JCC2 to become a cornerstone capability of the Cyber domain effects, and integration in larger Operations Plans and Campaign Plans across all eleven combatant commands.

3. SCOPE

The JCC2 Program Management Office will utilize this contract to support the Warfighter needs for operational expertise via program funded Field Application Engineers (FAE). Offices of the Secretary of Defense, Combatant Commands, Services, and other Agencies may choose to fund their own FAEs through this contract in 12-month increments. Rates for new FAEs may include additional cost as agreed upon with the funding element such as cost of living adjustments mandated for the area, travel, living or requisite insurance costs associated with the host location or site. FAEs provide on-site technical expertise in all aspects of JCC2 use and provide a direct conduit between the Government PMO and the Stakeholders within the Command they support.

The services required under this FAE contract include all disciplines required for JCC2 Software support at the Tier-1 level to include maintenance/sustainment of JCC2 systems in accordance with (IAW) applicable guidance, policies, and directives, . These services will be applied to all systems and activities within the JCC2 portfolio supporting mission operations locally and remotely.

The contractor shall support existing applications to include but not limited to JCO, JCC2-R, TASC, MADSS capabilities. JCC2 capabilities operate at the Unclassified, Secret, and Top-Secret classification domains.

The contractor shall provide sustainment support, documentation support (maintain and update JCC2 documents), admin training support, and other forms of support for JCC2. JCC2 is composed of Mission Applications, Cloud based infrastructure on which the Mission Applications run, which the Contractor shall provide necessary support for all applications on the infrastructures deployed.

4. Requirements and Description of Services

4.1. General Requirements

4.1.1. The contractor shall have subject matter expertise of USCYBERCOM and service cyber component network architecture, organizational structure of cyber defenders and assigned responsibilities, cyber sensors, and other critical defensive technologies, reporting requirements and processes.

4.1.2. A Field Application Engineer (FAE) provides technical support, product demonstrations, customization assistance, training, and feedback gathering for customers. They bridge the gap between customers and product development teams, ensuring effective product implementation, user assessments and customer satisfaction.

4.1.3. The contractor shall provide embedded FAE/JCC2 Capability SMEs to support the user community. These resources will be intentionally placed as directed by PMO to make the biggest impact. Once locations are selected, they will remain constant as primary locations, but the team will also travel to other secondary locations as needed to provide additional support. The contractor will receive guidance on primary locations prior to contract award to allow time for staffing in these locations.

4.1.4. 2.11.2. Contractor embedded FAE/JCC2 Capability SMEs shall consistently answer user questions with in-depth understanding of the mission and the capabilities to help the users best utilize the applications to support mission needs. The contractor embedded FAE/JCC2 Capability SMEs shall support resources with five (5) days onsite. The team will engage across sites as well as with the larger team to fully understand application(s) functionality for mission(s), trends and issues in the user community and strategize on how to best address any issues or concerns.

4.1.5. FAE/JCC2 Capability SMEs will serve as experts in all aspects of the operational and information environments, operational integration, and experienced within the Commands, and organizations they support. They provide onsite technical expertise, assistance, and training to the Commands they support as well as providing a valuable conduit between the Government PMO and the Commands/ Stakeholders they support. They integrate PMO capabilities with organizational data, systems, and processes within their Commands and provide expertise in integrating the entity they support with the capabilities of the JCC2 PMO.

4.1.6. The contractor shall support all three enclaves (NIPR, SIPR, JWICS) ensuring operational capability, security, and COOP capability supporting a one (1) hour recovery point objective.

> Note: This is expected to be an automated Amazon Web Service (AWS) failover process. However, some applications may react differently to infrastructure changes (e.g. one Domain Controller drops, and the application should automatically look to the secondary Domain Controller).

4.1.7. The contractor shall assist the government in identifying data and interface integration opportunities to deliver data products to the operational community. The contractor shall present any such opportunities to the PMO.

4.1.8. The contractor shall use JCC2 designated collaboration tools.

4.1.9. The contractor shall support PMO-driven sessions with operational users to identify capabilities needs and construct journey maps. The contractor shall deliver any resulting journey maps or associated documentation to the PMO.

4.1.10. The contractor shall provide technical support on the deployment, installation and troubleshooting of JCC2 applications as directed by JCC2 PMO. It is expected the contractor shall collaborate with third party contractor/developer SMEs who are directly supporting JCC2 suite of capabilities/applications development.

4.1.11. The contractor shall analyze requirements, software design documentation and UIX journey maps to cross reference custom features developed exclusively for other SCCs to reduce duplication and maximize reuse and ensure the JCC2 PMO is involved.

4.1.12. The contractor shall establish and report on metrics associated with operational utility and operationalization of JCC2 applications to inform design decisions and technical roadmaps.

4.1.13. The contractor shall support technical interchanges with operational stakeholders, to include but not limited to, elicitation, analysis, and system requirements management, ensuring traceability and alignment with system models. The contractor shall ensure that JCC2 is represented in all communications with operational stakeholders.

4.1.14. The contractor shall continuously monitor JCC2 software products into a multitude of classified and unclassified environments.

4.1.15. The contractor shall provide support to the JCC2 developmental and operational test agencies as directed. Field Applications:

Mission Applications	
Current	Description
Threat Hub	A tool that allows for the correlation of intelligence reporting within the DoD cyber landscape, enabling dynamic knowledge sharing though the use of Records or Intelligence Products for conducting and documenting investigations.
Triage	A tool that allows operators to configure detection filters based on threat signatures, cyber threat intelligence reporting, or custom expressions for authoritative alerting on BDP ingested cyber event data for automatic or manual elevation to incident responders to remediate.
Cyber Awareness Dashboard (CAD)	A tool that allows for the tracking, mapping, and risk scoring of vulnerabilities collated from different authoritative and contemporary DoD and open-source feeds fused into a single data model.
Aggress Assess, Inspect and Test (A2IT)	A tool that allows decision makers the ability to deconflict between Red Team activity with detected Red Report activity with high confidence to ensure

	appropriate response to noticed/reported network activities.
Cyber 9 Line (C9L)	A tool that allows for the quick communication of non-sensitive cyber incident information to U.S Cyber Command for unclassified information exchange to non-DoD elements to include state and county governments on reported cyber incidents.
Codex	A tool that allows the user to aggregate indicators of compromise across multiple disparate cyber threat intelligence sources, correlate the risks identified by each, and provides a composite risk score prioritizing DODIN threats for comparison and distribution across the DODIN enterprise.
Crucible	A tool that allows cyber analysts to automate the correlation of indicators of compromise detected within DODIN sensor and cyberspace operations data with context within their given areas of operation
Dispatch	A tool that allows users to generate and disseminate orders, and track near real-time compliance with the fix actions or get-well plans associated with each order and respective sub-taskings.
Rally	A tool that allows users to consolidate feeds related to incidents worked at various tiers, track ticket distribution among teams, and track near-real time metrics related to the incident handling process while remaining 6510 compliant to support exports to the Joint Incident Management System (JIMS)
SIGACT	A tool that allows a user to build out a comprehensive report to provide information on enemy, suspected enemy, and anomalous activity, referred to as Significant Activity, on DOD networks that are shared across systems and DOD services via the BDPs.
UNITY	A tool that allows an analyst to explore the BDP(s) data store on DODIN and cyberspace operations to find or hunt for discrete finding(s).
REDMAP	A tool that allows analysts and decision-makers to visualize active vulnerabilities to critical assets on a map that focuses customized high priority alerts by mission or named area(s) of interest allowing for rapid adjudication and response.
Record Service	A distributed service standardized to collaborate on, synchronize, and publish products across different DoD services, fabrics, applications, and systems.

Asset Service	A customizable service that centralizes and synthesizes knowledge of DoD assets on the local BDP instance with current work to make it a distributed service.
Notification Service	A BDP level service that alerts users when a product is created, or a workflow progresses regardless of which JCC2 application you are in.
Scoring Service	A distributed service that generates, updates, and distributes scores for entities seen in the data regardless of the BDP instance.
Observable Service	A service that monitors entities active in reporting and sensor data.
Signature Service	A service that curates and intelligently shares alert-generation signatures.
Research Service	A service that creates/maintains as collaborative wiki for documenting adversary capabilities.
Order Service	A service that allows for the assigning of workflows to specific users and/or teams.
Directory Service	A BDP level service that allows for user identification, user groups, and appropriate permissions (Need-to-know, referred to as authorizations) to view data and access to various BDP applications
Joint Cyber Operations	
JCC2-R	
Mission Assurance Decision Support System (MADSS)	

4.2. Training

The contractor shall develop an overall operator training program and, shall conduct training as required and as requested by the Government. This training shall include "hands on" user interface training on the use of the JCC2 capabilities.

The contractor shall develop courses as final and complete training products

The contractor shall provide all course materials for courses presented by contractor.

The contractor shall provide course materials electronically for each trainee. Final and any

updated course materials shall be turned over to the Government electronically to be used for follow-on training. The contractor shall provide courseware and instructional material in a format to allow follow-on training and maintenance by operators.

The contractor shall provide a course survey for each trainee to be completed at the conclusion of each course that rates the effectiveness of the training and deliver completed surveys to Government Representative, COR and PM within 5 calendar days from course completion.

4.2.1. The training scope includes maintaining the currency of established new user training (guides, videos, etc., differences training for new features, analytics user guides, and general training.

4.2.2. The contractor shall support agile virtual and on-site training and exercise support, as required/directed. All training shall be coordinated and approved with the JCC2 PMO offices prior to schedule and execution.

4.2.3. As directed by the Government, the contractor shall provide training materials for use in formal Cyber Initial and Mission Qualification Training courses (IQT and MQT).

4.2.4. Training shall be delivered in the format that works best for the trainees, including in-person and virtual live training, or other delivery options as agreed by the Government. Plans for new training shall be submitted to the Government for prior approval and include the following: customer training requirements, student learning objectives, a basic instructor lesson plan, student guides or materials (as needed) and required visual aids and a sample student feedback form (for in-person or virtual live led training only)

4.2.5. On-demand training materials (including but not limited to user guides, videos, etc.) shall be posted in the JCC2 directed location(s) within 10 days of completion of training IAW CDRL AXXX, Training Materials and Course Feedback.

4.2.6. Within 10 days of class end date, for in-person and virtual instructor-led training only, the contractor shall provide PMO with copies of student critiques, along with a brief, one-page summary cover sheet noting any significant trends, recommended course improvements and an average overall student course rating based on a 5.0 scale IAW CDRL A006, Training Materials and Course Feedback.

4.2.7. The contractor shall develop and sustain interfaces and exchange information with the Persistent Cyber Training Environment (PCTE) for training of JCC2 applications.

4.2.8. The contractor shall develop, deploy, and update training material

4.2.9. The contractor shall provide a minimum of 12 virtual/in person training sessions over the course of 12 months from the date of funding obligation.

4.2.10. The contractor shall coordinate and get PMO approval prior to all training sessions.

4.2.11. The contractor shall build out training materials and a curriculum to facilitate education of the service cyber components and JCC2 capability adopters.

4.2.12. The training materials created from this effort shall be shared throughout the federal and state government and will be uploaded to each BDP to further expand on the operator’s knowledge base, with coordination of the Service BDPs Program Managers.

4.2.13. The trainers will focus on creating a joint curriculum, tailoring it to Service level implementations, and providing live training sessions to ensure an expansive but effective training reach.

4.2.14. Trainings provided will include Train-the-Trainer (T3) training and operator training.

4.2.15. In-person training and users will be located at sites determined by the JCC2 PMO and may include but not limited to AFCYBER, ARCYBER, USINDOPACOM, NORTHCOM, USSOCOM, USSOUTHCOM &JFHQ-DODIN.

4.2.16. Contractor shall provide an appropriately sized training team for the requirements outlined in thisSOW.

The contractor shall collaborate and coordinate training material across the JCC2 enterprise **which will involve interfacing with JCC2 engineers, engineers from various JCC2 data source systems, other contractor SME's, as directed by the PMO.**

5. Team Composition and Special Qualifications

Section 5 addresses Team composition, estimated level of effort and special qualifications.

5.1. Team Composition and Special Qualifications

5.1.1. General Requirements

The list of requirements detailed in this section changes frequently to meet emerging requirements and priorities established by the operational community due to the continuously evolving cyber threat and the variety of techniques used by cyber adversaries along with the maturation of cyber C2 concepts of employment with the joint community. As a result, these requirements are representative, but not comprehensive.

4.1.2.1 The contractor shall demonstrate their ability to respond to the changing environment through its proposed staff training programs.

4.1.2.2 The contractor shall fill key positions, at the locations identified, with the clearances, qualifications, and access required to fulfil this contract within 15 business days of the contract award date.

4.1.2.3 Key positions cannot be dual-hatted.

4.1.2.4 Residual billets must be filled within 20 business days of contract award date.

4.1.2.5 One means of demonstrating this ability is to furnish sanitized resumes, or acceptable evidence of qualifications of the individuals the contractor would place into each of the positions.

The following section describes the services for JCC2 FAE. The government approach to team composition is to construct each development team as an integrated product team that excels in requirements gathering, decomposition, prioritization, , deploying, and sustaining feature deliveries.

4.1.2.6 The contractor shall support operationalization of JCC2 apps on all 3 domains.

4.1.2.7 The contractor shall be responsible for the employment, guidance, supervision, and training of all personnel assigned to perform tasks under this contract.

Anticipated contractor tasks include but are not limited to technical requirements listed in section 3.

A list of contractor deliverables is below. Please note, the paragraph referenced in the IDIQ DD Form 1423 will not map to a paragraph in this document.

Table 1: JCC2 required CDRLs

CDRL	Description	Document Number	Frequency
A001	Monthly Status Report	DI-MGMT-80368A	Monthly for the Period of Performance
A002	Financial Reports		Monthly for the Period of Performance
A004	Briefing Material	DI-MGMT-81605	As Required, submission will be NLT 7 days prior to the conference/event to include but not limited to: Kick-off meeting Minimum of one (1) event during the period of performance
A005	Meeting Minutes	DI-ADMN-81505	As Required. Meeting minutes are due NLT 10 days after conference/event/ comments to include but not limited to: Kick-off meeting.
A006	Training Materials		Monthly for the Period of Performance
A009	Contractor's Corrective Action Plan		

5.2. Level of Effort

Table 2: Level of Effort – JCC2 AEs (20 FTE's)

JCC2 Battle Management Support Capability					
FTE Requirement	**Qty**	**Hours**	**Performance Location**	**Cert/Experience/Clearance**	**Key Position**

Operational Program Manager, Senior	5	9,400	Vendor Location	TS/SCI	Key (x5)
Field Application Engineering	15	28,200	San Antonio, TX	TS/SCI	Key (x10)

5.3. Security Clearances

5.3.1. Facility Security Clearance. The work to be performed under this contract/order is up to the Top-Secret level and will require Sensitive Compartmented Information (SCI) access eligibility for some personnel including CI-polygraph to obtain a USCYBERCOM and/or National Security Agency (NSA) retention badge. The contractor shall require access to NIPRNet, SIPRNet, JWICS, and potentially NSANet.

5.3.2. All Contractor personnel assigned to work on classified activities shall be cleared at the Top Secret/Sensitive Compartmented Information (TS/SCI) level clearance in accordance with "Personnel Security Requirements for Contractor Access to NSA/CSS Sensitive Compartmented I (Attachment to DD 254)". Fully unclassified development efforts may be performed by uncleared personnel.

5.3.3. Contractor personnel without a security clearance may perform unclassified tasks. However, non-U.S. citizens, to include immigrant aliens, are not authorized access to any portions of this contract or to commence performance of any work under this contract without express written approval from the Contracting Officer. In accordance with the conditions as prescribed by 352.204-9014, NOTIFICATION OF NON-U.S. CITIZEN PARTICIPATION, the contractor shall provide all the requested information for processing of each non-U.S. citizen seeking access to or being proposed to perform work on this contract.

5.3.4. Security will be addressed IAW the DD254.

5.3.5. Information Subject to Export Control Laws/International Traffic in Arms Regulation (ITAR) Public Law 90-629, “Arms Export Control Act,” dated 26 Dec 2013, as amended (22 U.S.C 2751 et. Seq.) requires that all unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license under EO 12470 or the Arms Export Control Act, Continuation of Export Control Regulations, dated 30 Mar 1984, and that such data required an approval, authorization, or license for export under EO 12470 or Arms Export Control Act. For purposes of making this determination, the Militarily Critical Technologies List (MCTL) shall be used as general guidance. All documents determined to contain export controlled technical data will be marked with the following notice:

WARNING: This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate IAW provisions of DoD Directive 5230.25, “Withholding of Unclassified Technical Data from Public Disclosure, 06 Nov 1984

Incorporating Change 1, dated 18 Aug 1995".

5.3.6. Facility Security Clearance. The work to be performed under this contract/order is up to the Top-Secret level and will require Sensitive Compartmented Information (SCI) access eligibility for some personnel including polygraph to obtain a USCYBERCOM and/or National Security Agency (NSA) retention badge. The contractor shall require access to NIPRNet, SIPRNet, JWICS, and NSANet.

5.3.7. All Contractor personnel assigned to work on classified activities shall be cleared at the Top Secret/Sensitive Compartmented Information (TS/SCI) level clearance in accordance with "Personnel Security Requirements for Contractor Access to NSA/CSS Sensitive Compartmented I (Attachment to DD 254)". Individuals possessing a current Counterintelligence (CI) polygraph will be considered for a contract position that requires a full-scope polygraph if they possess a Conditional Certification of Access (CCA) pending the successful completion and adjudication of a full-scope polygraph. Fully unclassified development efforts may be performed by uncleared personnel.

5.3.8. Contractor personnel without a security clearance may perform unclassified tasks. However, non-U.S. citizens, to include immigrant aliens, are not authorized access to any portions of this contract or to commence performance of any work under this contract without express written approval from the Contracting Officer. In accordance with the conditions as prescribed by 352.204-9014, NOTIFICATION OF NON-U.S. CITIZEN PARTICIPATION, the contractor shall provide all the requested information for processing of each non-U.S. citizen seeking access to or being proposed to perform work on this contract.

5.4. Minimum Skills, Experience, and Certifications

Table 3: Required Certifications and Experience

Title	Clearance & Required Certifications	Experience
Operational Program Manager, Senior	TS/SCI, Project Management Professional (PMP) (PMI-ACP is desirable), SAFe SA	Program Manager – Senior Represents JCC2 PMO in all local stakeholder engagements and is primary point of contact to JCC2 program office for communications with supported units and lead for assigned JCC2 projects. Responsible for the operational planning, establishment, execution, and evaluation of a multifaceted program/project. Responsible for fiscal, operational, administrative, and human resources management of the program; serves as principal point of representation for JCC2 PMO and liaison with external constituencies on

		operational matters and provides day-to-day professional guidance and leadership as appropriate to the area of expertise. Develops detailed work plans, schedules, project estimates, resource plans, and status reports. Conducts project meetings and is responsible for project tracking and analysis. Ensures adherence to JCC2 PMO directives and quality standards and reviews project deliverables. Manages the integration of vendor tasks and tracks and reviews vendor deliverables. Recommends and takes action to direct the analysis and solutions of problems. At least 10 years of overall experience in the functional area. A bachelor's degree in related field required. Master's degree may substitute for 2 years of experience. Five years of relevant experience, experience leading complex DevSecOps programs with an emphasis on cloud, cyber and platform technologies. Three years' experience managing subcontractors and projects using agile, and/or spiral development models. Required Qualifications • Project Management experience or equivalent field • Scaled Agile Framework (SAFe) Agile Certification • Broad understanding of operational cyber landscapes • Practical experience using JIRA and Confluence for project management Desired Qualifications:

		• Certified Information Systems Security Professional (CISSP) Certification • Programming and query language experience • Strong project management skills with experience in DevOps and/or SAFe/Agile • Atlassian Collaboration tools • AWS SysOps Administrator certification • Red Hat certification Government or military cyber experience
Field Application Engineer	TS/SCI, Security +	Provides subject matter proficiency for work described in the task. Responsible for providing analytical skills to support process improvement, specialized studies, and definition of requirements. Provides customer support through the performance of on-site installation, as well as overseeing any necessary diagnoses, troubleshooting, service, and repair of systems. Requires an understanding of the Cyber Mission Force (CMF) organizational construct, tools/capabilities utilized in cyberspace operations, and experience in system/network administration, incident response, and forensic analysis. Participates in the establishment measurement, and achievement of customer satisfaction metrics. Performs project management function from client engagements to include identification, scheduling, tracking, and reporting. Provides client feature request to the JCC2 PMO and project support personnel. Develops and writes documentation as required. Train and familiarize operators on equipment and systems as directed by the JCC2 PMO. Supports an environment conducive to successful team interaction and customer

		satisfaction. Possesses strong, results-oriented work ethic and customer service orientation. Required Qualifications: • Ability to conduct database queries • Ability to travel greater than 25% • Current secret clearance with ability to attain a TS/SCI clearance and willing to obtain a polygraph. • 5 years experience in working in Cyber Mission Force community. • At least 10 years IT systems administrative experience with both Microsoft and Linux platforms. With two years proficient understanding of maintenance (patching, STIG, and upgrade processes) on AWS cloud infrastructure. • Demonstrated experience and/or training in system administration and development best practices in AWS Desired Qualifications: • Programming and query language experience • Strong project management skills with experience in DevOps and/or SAFe Agile • Atlassian Collaboration tools • AWS SysOps Administrator certification • Red Hat certification • Government or military cyber experience

6. Contractual Requirements

6.1. Staffing

Table 5: Staffing Timeline Requirement

Required Date	Positions Filled
10 Business Days after Contract Award date	50% of Key positions filled
15 Business Days after Contract Award date	100% of Key positions filled

20 Business Days after Contract Award date	100% of all Positions filled

6.2. Key Personnel

The Government has determined the following positions to be Key Personnel essential to the performance of this task order (See table 4.1.1). All Key Personnel require a Top Secret SCI level clearance upon start of Task Order. If any Key Personnel need to be replaced during the PoP, the contractor shall propose a replacement individual of equal or greater experience upon for government approval, provide a sanitized resume (no names or other data that would identify the specific individual) to the Contracting Officer and COR for review. Key Personnel may not be "dual- hatted" in technical positions.

FIELD APPLICATIONS ENGINEER					
FTE Requirement	**QTY**	**Hours**	**Performance Locations**	**Cert/Experience/ Clearance**	**Key Posiiton**
Field Application Engineer	18				
Product Trainer, Senior	1	1880			
Technical Program Manager, Senior	1	1880			

6.3. Performance Reporting

The contractor's performance will be monitored by the Government and reported in the Contractor Performance Assessment Reporting System (CPARS). Performance standards shall include the contractor's ability to:

- Provide quality products, incidentals, and customer support
- Provide satisfactory new products, product repairs or advance replacements, as appropriate
- Provide timely and accurate reports
- Respond to the customer's requirements as identified
- Meet subcontracting goals if applicable

6.4. Program Management / Project Management

6.5. The contractor shall provide and maintain comprehensive, pro-active, integrated program management that focuses on meeting or exceeding government requirements and ensures compliance with all mandatory, statutory, and regulatory requirements.

6.6. Contractor shall provide management, supervision, personnel, and technical and logistical support functions in support of the JCC2 program and product technical responsibilities. The Contractor shall perform administrative, technical, and financial management function during the course of this effort and shall maintain a status of their effort towards achieving the objectives, including all technical activities and efforts,

problems/deficiencies, impacts, and recommended solutions. The contractor shall provide briefing and capability demonstration assistance to the assigned locations.

6.7. 2.1.2. The contractor shall provide for an electronic exchange of information and deliverables to the government. The contractor shall coordinate with the Program Manager (PM) or submit the deliverable electronically to the Contracting Officer (CO), PM, Contracting Officer's Representatives (COR). When sending Microsoft Access, Visio, or Project files, also submit an Adobe PDF version. If deliverables exceed five (5) megabytes the contractor shall distribute them through DoD SAFE - https://safe.apps.mil/.

6.8. 2.1.3. The contractor shall provide a Status Report monthly. The contractor shall document the progress of work, status of the program, and document existing or potential problem areas. The monthly reports are due on the fifth calendar day of each month (Deliverable: Monthly Status Report).

7. Contractor shall provide training documentation:

• Final draft review 3 months prior to PoP.

• Final Version delivered electronically and saved on Govt shared drive 1 month prior to PoP for follow-on training.

7.1.

7.1.1. Field Application Engineers (FAEs) are a critical component of the JCC2 program. They are experts in all aspects of the operational and information environments, strategic and operational integration, and experienced within the commands, and organizations they support. They provide on-site technical expertise, assistance, and training to the Commands they support as well as providing a valuable conduit between the Government PMO and the Commands/ Stakeholders they support. They assist in the creation of best practices, draft and document Command tactics, techniques, and procedures (TTP) and standard operating procedures (SOP), integrate JCC2 capabilities with organizational data, systems, and processes within their commands and provide expertise in developing new test cases, and testing new features.

7.1.2. The Contractor shall provide qualified FEAs at the eleven (11) Combatant Commands, Service Cyber Components as necessary, and the Joint Staff under this Task Order beginning at an agreed upon date for the duration of this contract.

7.1.3. The Contractor may be tasked to provide qualified FAEs under separately funded efforts through this Task Order and as agreed upon by both parties.

7.1.4. The Contractor and the Government will agree to any additional costs such as mandated cost of living adjustments, travel, living or requisite insurance costs associated with the host location, nation, or site.

7.1.5. The Contractor will provide FAEs with the appropriate security clearances for access to the supported Government site. The Government agrees to provide security clearance requirements prior to entering into any agreement as part of this Task Order.

7.1.6. The Government PMO, in coordination with the Contractor will be responsible for administrative actions necessary to support base access such as Common Access Card (CAC), Synchronized Pre-deployment and Operational Tracker (SPOT) orders, and the overseas Contractor approval process commonly known as European Contractor Online Processing System (ECOPS).

7.1.7. The Government site Sponsor, in coordination with the PMO and Contractor will be responsible for providing site access necessary to perform the requisite work in support

of the Command.

7.1.8. FAEs are responsible for all aspects of JCC2 integration into the command processes as needed by the Government sponsor including, but not limited to, Battle Rhythm events integration, documentation, and facilitating Government PMO engagements.

7.1.9. FAEs are responsible for supporting on-site and virtual training, training programs, development of Tactics, Techniques, and Procedures (TTP), and SOP within the Commands. Training or engagements that require off-site support will be coordinated through the Government PMO.

7.1.10. FAEs support the program as the first responders for any issues regarding JCC2 access or functionality by users within their Commands IAW with the Service Level Agreement (SLA) agreed upon by both parties.

7.1.11. FAEs are responsible for supporting Command implementation of JCC2 in support of mission planning, execution, and assessment in support of campaign plan objectives.

7.1.12. FAEs are responsible for supporting JCC2 testing within the Command enterprise architecture and documenting deficiencies and anomalies.

7.2. Reporting

7.2.1. Provide programmatic reporting to inform Government PMO decision making and oversight.

7.2.2. The FAEs will provide a Weekly Activity Report (WAR) in an agreed upon format, no later than 1200 Central U.S. Time on Friday to the Government containing a summary of activities, upcoming key events and engagements, training/trained personnel and any scheduled out of office time.

7.2.3. The Contractor shall provide a Monthly Activity Report (MAR) by the 10th calendar onboarding and training status of all FAEs, FAE activities by Command including Sponsor contact information, engagements, training, any scheduled out of office time. (CDRL A001) day of the following month that provides a summary of overall GIO support activities,

7.2.4. The Contractor shall provide a complete list of all personnel supporting this contract who require government issued credentials. Changes in the status (hired, resigned, reassigned, etc) shall be reported to the Government within 10 business days.

7.3. Configuration and Data Management

The contractor shall establish, maintain, and administer an integrated data management system for collection, control, publishing, and delivery of all program documents.

The data management system shall include but not be limited to the following types of documents: CDRLs, White Papers, Status Reports, Audit Reports, Agendas, Presentation Materials, Minutes, Contract Letters and Task Order Proposals. The contractor shall provide the Government with electronic access to this data, including access to printable reports.

7.4. Records, Files, and Documents

All physical records, files, documents and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this SOW, maintained by The contractor which are to be transferred or released to the Government or successor contractor, shall become and remain Government property and shall be maintained and disposed of IAW Air Force Manual (AFMAN) 33-363, Management of Records; AFI 33-364, Records Disposition – Procedures and Responsibilities; the Federal Acquisition Regulation, and/or the Defense Federal Acquisition Regulation Supplement, as applicable. Nothing in this section alters the rights of the Government or The contractor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this SOW or the NetOps and Infrastructure Solutions contract of which this SOW is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

7.5. Security Management

7.5.1. The Contractor will comply with DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM), for the safeguarding of classified information.

7.5.2. The Contractor will comply with DoDI 5200.48, Controlled Unclassified Information, AFI 16-1404 Air Force Information Security Program, and Air Force Guidance Memorandum 2020-16-01, Air Force Guidance Memorandum for CUI, 23 Jul 20. The Contractor shall consult the applicable security classification guide to monitor CUI aggregation for potentially generating classified information by compilation.

7.5.3. The Contractor will comply with DoDM 5400.07/Air Force Manual 33-302, DoD Freedom of Information Act (FOIA) Program requirements.

7.5.4. Protection of CUI and unclassified DoD information not approved for public release on non-DoD Information Systems (IS) will be protected IAW DoDI 8582.01, Security of Non- DoD Information Systems Processing Unclassified Nonpublic DoD Information. Unless specific categories of CUI require more stringent controls, non-DoD IS must be protected using the guidelines set forth in NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

7.6. Personnel Security

Individuals performing work under this task order shall comply with applicable program security requirements as stated in the task order. All personnel shall possess the clearances required at the time they report for work on a Team.
The Contract Security Classification Specification (DD Form 254) will be at the basic contract and task order level and will encompass all security requirements.
All contractors located on military installations shall also comply with Operations Security (OPSEC) requirements as set forth in DoD Directive 5205.02, Operations Security Program and AFI 10-701, Operations Security. IAW DoD 5200.2-R, Personnel Security Program (Jan 87), DoD military, civilian, consultants and contractor personnel using unclassified automated information systems, including

e-mail, shall have, at a minimum, a completed favorable National Agency Check plus Written Inquiries (NACI).

7.7. Protection of System Data

Unless otherwise stated in the Task Order, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network IAW all applicable policies and procedures for such data, including DOD Regulations 5400.7-R and DoDM 5200.01 to include latest changes and applicable service/agency/combatant command policies and procedures. The contractor shall protect system design related documents and operational data at least to the level provided by Secure Sockets Layer (SSL)/Transport Security Layer (TSL)-protected web site connections with certificate and or user id/password-based access controls. In either case, the certificates used by the contractor for these protections shall be DoD- or Intelligence Community (IC)-approved PKI certificates issued by a DoD or IC approved External Certification Authority (ECA) and shall make use of at least 128-bit encryption.

7.8. Travel Requirements

7.8.1. Travel may be required during the performance period of this contract at the request of the Government and within the Continental United States (CONUS) and Outside the Continental OCONUS. A Status of Forces Agreement (SOFA) may be required at designated sites in OCONUS. Dates and destinations are not available currently. The Contractor will utilize the following procedures:
Submit a written request to proceed with travel to the COR six (6) weeks prior to travel or as soon as identified except when an operational exemption applies. Contractor will not travel until authorization from COR is received. Arrange transportation and other travel-related requirements to ensure attendance by appropriate Contractor personnel at the best value for the Government and in accordance with FAR 31.205-46, Travel Costs. The website for per diem rates is:
http://www.defensetravel.DOD.mil/ Travel will be reimbursed on a cost basis; no profit or fee will be paid.

6.12.2 Travel Reports will be submitted to the COR five (5) business days after trip completion and will be submitted IAW CDRL A010 RECORD OF MEETING MINUTES AND TRIP REPORTS. Travel Report format will include at a minimum the following: dates of travel, destination, purpose, individuals traveling, research on airfare, hotel, car rental & per diem, and issues and challenges, recommendations, and a signature

7.8.2. All Visit Access Requests (VARs) will be submitted in writing to the Government PMO NLT 72 hours prior to travel except when an operational exemption applies.

7.9. Place and Period of Performance (PoP)

7.9.1. Period of Performance. The total PoP for this Task Order is 36 months which includes a 12-month base with two 12-month options. Optional FAEs are funded in 12-month increments unless otherwise specified in the agreement.

7.9.2. Place of Performance. When this Task Order requires the contractor to work in a Government facility, the Government will furnish or make available working space, network access and equipment to include:

- Windows PCs with Microsoft Office Suite (Outlook, Word, Excel, PowerPoint, etc.) with access to NIPRNet, SIPRNet and JWICS enclaves
- Telephone (local/long distance calls authorized as dictated by Task Order performance requirements)
- Facsimile
- Copier
- Printer
- Digital Scanner

7.9.3. The places of performance for this contract are permitted at the Contractor facilities and the following Government facilities. Refer to the DD254 for additional locations.

4.1.2.1 AFLCMC/HNC (JBSA – Lackland AFB TX)
4.1.2.2 USAFRICOM (Kelley Barracks, Stuttgart GE)
4.1.2.3 USCENTCOM (MacDill AFB, Tampa FL)
4.1.2.4 USCYBERCOM (Ft. Meade, MD)
4.1.2.5 USEUCOM (Patch Barracks, Stuttgart GE)
4.1.2.6 USINDOPACOM (Camp Smith, Honolulu HI)
4.1.2.7 JOINT STAFF (Pentagon, Arlington VA)
4.1.2.8 USNORTHCOM (Peterson AFB, Colorado Springs CO)
4.1.2.9 USSOUTHCOM (Doral, FL)
4.1.2.10 USSOCOM (MacDill AFB, Tampa FL)
4.1.2.11 USSPACECOM (Peterson AFB, Colorado Springs CO)
4.1.2.12 USSTRATCOM (Offutt AFB, Omaha NE)
4.1.2.13 USTRANSCOM (Scott AFB, St. Louis MO)
4.1.2.14 AFCYBER Headquarters (JBSA – Lackland TX)
4.1.2.15 ARCYBER Headquarters (Ft Gordon, GA)
4.1.2.16 Other locations as directed by the Government

During the performance period of this contract at the request of the Government and within the Continental United States (CONUS) and Outside the Continental OCONUS. A Status of Forces Agreement (SOFA) may be required at designated sites in OCONUS.

7.10. Normal Hours of Operation

JCC2 is operational 24x7 and support under this Task Order must ensure the system is available to support operational requirements. The average work week is 40 hours. The average workday is 8 hours with Core hours 9am to 3pm Monday through Friday. Contractor personnel shall be scheduled to support the ticket resolution timelines and maintenance activities during ASIs as identified by the JCC2 PMO. During duty hours, contractor must respond within the timelines necessary to support the resolution timelines as directed by the government

7.11. Billable Hours

In order for man-hours to be billed, deliverable services must have been performed in direct support of a requirement in the SOW. In the course of business, situations may arise where Government facilities may not be available for performance of the Task Order requirements (i.e., base closure due to weather, Force Protection conditions, etc.) and contractor personnel could be assigned elsewhere (to work) in the organization. If the base is officially closed, the Contractor is expected to telecommute or work out of the local office in order to meet JCC2 mission requirements. When a building is closed, the contractor shall contact the CO for direction. There may also be occasions when support contractors are invited to participate in morale and recreational activities (i.e., holiday parties, golf outings, sports days and other various social events). Contractor employees shall not be directed to attend such events by the Government. Since a contract employee is not a Government employee, the contract employee cannot be granted the same duty time activities as Government employees. Participation in such events is not billable to the Task Order and contractor employee participation should be IAW the employees' company's policies and compensation system.

7.12. Contractor Identification

All contractor/subcontractor personnel shall be required to wear AF-approved or provided picture identification badges so as to distinguish themselves from Government employees. When conversing with Government personnel during business meetings, over the telephone or via electronic mail, contractor/subcontractor personnel shall identify themselves as such to avoid situations arising where sensitive topics might be better discussed solely between Government employees. Contractors/subcontractors shall identify themselves on any attendance sheet or any coordination documents they may review. Electronic mail signature blocks shall identify their company affiliation. Where practicable, contractor/subcontractors occupying collocated space with their Government program customer should identify their workspace area with their name and company affiliation. Refer to Clause H063 of the overarching ID/IQ contract.

7.13. Training

Contractor personnel are required to possess and maintain the skills necessary to support their company's minimum requirements of the labor category under which they are performing.
Training necessary to meet minimum requirements will not be paid for by the Government or charged to the task order by contractors. All training shall be current with the services offered throughout the life of the contract Task or Delivery Order.

7.14. Quality Process

As a minimum, the prime contractor shall be appraised at CMMI Development or

Services Level IV using the Software Engineering Institute (SEI) SCAMPI by an SEI-authorized lead appraiser for the entire performance period of the contract, inclusive of options. Acceptable System Engineering processes shall be maintained for the entire performance period of the contract, inclusive of options.

7.15. Supply Support

In situations where the purchase of new COTS software is needed to satisfy the requirements of a particular task order, the contractor shall use available existing enterprise licenses. If enterprise licenses are unavailable, then products will be obtained via the DoD Enterprise Software Initiative (ESI) Blanket Purchase Agreements (BPAs). If products are unavailable from ESI, then products will be acquired through the NETCENTS-2 Products contract IAW DFARS 208,74 and FAR 51.101. The updated listing of COTS software available from DoD ESI sources can be viewed on the web at: http://www.esi.mil.

The contractor shall use COTS and Government Off-the-Shelf (GOTS) HW/SW, and firmware purchased from original equipment manufacturers (OEMs) and their trusted distributors, no 3rd party companies. The contractor shall ensure their supply chain risk management plan for provisioning of supplies and services to the Government IAW DFARS 252.239-7018, NIST Cybersecurity Framework 800- 161 and International Organization of Standards (ISO) 55001:2014 and 19770-1:2017.

The contractor shall ensure PMO identified personnel are provided access to all SW and HW accounts and list the applicable PMO as the Government owner.

The Contractor shall ensure compliance with DFARS 252.246-7007 “Contractor Counterfeit Electronic Part Detection and Avoidance System (AUG 2016)” and DFARS 252.246-7008 “Sources of Electronic Parts (AUG 2016)” in making purchases. Reporting of suspect counterfeit material to the Government-Industry Data Exchange Program (GIDEP) reporting system.

7.16. Government Provided Property, Facility, and Information (GFP, GFF, GFI)

When this Task or Delivery Order requires the Contractor to work in a Government facility, the Government will provide access to facilities, equipment, and technical information as required for the performance of this task. The Government will provide adequate working space to include, but not be limited to, computer server access and telephone access. Common Access Card (CAC) and facility access badges will be provided for individuals requiring regular access to Government facilities and computer systems. Copies of required Government furnished materials cited in the Task Order will be provided to the Contractor in hard or soft copy. All materials will remain the property of the Government and will be returned to the responsible Government COR upon request or at the end of the Task or Delivery Order PoP.

Government furnished property (GFP) issued to the contractor in support of the program requirements, are managed by the contractors in accordance with DFARS 52-245-1, 252.245- 7001-7004, 252.246-7000 and industry best practices. Government property that is incidental to the place of performance, remains accountable to the Government and is not considered GFP.

The contractor is responsible for any hardware installation driven by software requirements. In the Operational environment, the contractor, upon delivery of operationally approved software along with necessary hardware, shall coordinate with the operational maintenance support contractors along with outside vendors deemed necessary and related to the applicable products(s) as defined in the Task Order. In those instances, the DD Form 254 (DoD CONTRACT SECURITY CLASSIFICATION SPECIFICATION) requirements will be addressed in the individual Task Order and only at the security level necessary.

The Government will provide the development environment, but (unless they are required to be on a government network for software or product delivery for instance) the vendor will supply end user devices (laptop, desktop computing capability) used for day-to-day development.

Those devices shall meet Air Force cybersecurity requirements at the appropriate level - NIPR, SIPR, JWICS.

7.17. Contractor Computing Environment

Where GFE is not provided, the Contractor will provide and maintain in accordance with government standards, developer computing equipment required to accomplish the tasks in this activity.

7.18. Associate Contractor Agreement

Within 60 calendar days of contract start date, the contractor shall establish Associate Contractor Agreement (ACA) between contractors working on government contracts or projects that specify requirements for them to share information, data, technical knowledge, expertise, or resources. These requirements include maintenance/sustainment of COTS, GOTS and Open Source SW and HW.

8. PROGRAM PROTECTION

8.1. Operational Security (OPSEC)

8.1.1. IAW applicable security classification guidance and other applicable Government instructions, the Contractor shall develop and implement physical, personnel, and information security programs necessary to protect against the inadvertent disclosure of For Official Use Only (FOUO), Controlled Unclassified Information (CUI), and classified information pertaining to the JCC2 program.

9. Deliverables

9.1. The following table of CDRLs is provided for reference. See DD Form 1423-1's for detailed information regarding each deliverable.

A001	Monthly Activities Report	The 10th calendar day of each month or as agreed upon by both parties	Comprehensive report covering the Operational Activities report of FAE activities conducted during the previous month.