NETCENTS-2 SOLUTIONS
NetOps and Infrastructure Solutions – Full & Open (F&O)/Small Business (SB) Companion

45th Operations Group Combat Development Division
Information Systems Security Engineer (ISSE) Service Support
Task Order Performance Work Statement

Name:	[redacted]
Organization:	45th Operations Group, Combat Development Division (45 OG/CDD)
Address:	10351 Samuel C Phillips Pkwy Bldg 85125 (CCAFS) Patrick AFB 32925

All questions may be submitted in writing to the Contracting Officer via email at [redacted] with a copy to the Contract Specialist at [redacted].

Executive Summary

The 45 Operations Group Combat Development Division (OG/CDD) has several systems that will require cyber accreditation and are at various stages of development. The systems will be operated on Cape Canaveral Air Force Station (CCAFS) and Patrick Air Force Base (AFB). To accomplish the objectives of these projects, cyber accreditations must be achieved in accordance with Department of Defense (DoD) Instruction (DoDI) 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT). The establishment and maintenance of cybersecurity support, while ensuring adherence to applicable U.S. Air Force, and DoD Directives, Instructions, Guides, and Publications for these projects, is integral to obtaining cybersecurity certifications, including, but not limited to, Authorization to Operate (ATO). Cybersecurity requirements are shown in various National Institute for Standards and Technologies (NIST) Special Publications and National Defense Authorization Act (NDAA) 233 with 45 OG/CDD as the focal point for this effort.

45th Operations Group Combat Development Division
Information Systems Security Engineer (ISSE) Service Support
Task Order Performance Work Statement

1. Purpose

This task will provide on-site support of an Information Systems Security Engineer (ISSE) to support Information Assurance and Assessment (IA&A), Security Change Notices (SCNs), security tests and evaluations (ST&E), Authorizations to Connect (ATC), System Validation Authorization to Operate (ATO), and Interim Authorizations to Test (IATT) activities for Combat Development Division – Eastern Range (CDD-ER) systems. Tasks will include:

- Develop RMF artifacts in support of acquiring approvals for ATCs, IATTs, and ATOs for CDD-ER systems under development
- Deliver RMF artifacts to the CDD-ER for inclusion in RMF packages
- Provide recommendations for Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) implementation and risk mitigations, using cybersecurity training and experience, to the CDD-ER
- Maintain persistent lines of open communication with development engineers and support personnel within the CDD-ER for accurate portrayal of systems within artifacts and to ensure awareness of completion status and timelines
- Support the execution of Vulnerability and Compliance scanning of CDD-ER systems
- ISSE shall ensure system development follows the RMF 6 Step process IAW DoDI 8510.01

These tasks will include RMF assessment and cybersecurity control selection and Plan of Action & Milestone (POA&M) development support IAW Federal Information Processing Standards (FIPS), security Categorization and Control Selection for National Security Systems (CNSSI) 1253, and NIST publications, DoD and Air Force directives, policies, guidance, and instructions. It includes but is not limited to the NIST Special Publications 800-37 Guide for Applying the RMF to Federal Information System, and 800-53 Security and Privacy Controls for Federal Information Systems and Organizations.

2. Scope

The contractor shall designate an ISSE who shall be responsible for the control and coordination of all work performed on this task order.
The Contractor shall provide on-site support to complete Cyber accreditation artifacts/documentation, scans and analyses required to achieve cybersecurity accreditation from the Air Force Authorizing Official (AO).

2.1 Place of Performance and OPSEC Requirements

All activities will take place at either Cape Canaveral AFS or Patrick AFB. All contractors located on military installations shall comply with the following OPSEC requirements:

1. The contractor shall appoint in writing a point of contact to liaise with the OPSEC SM or coordinator.
2. The contractor shall develop an OPSEC program plan to address how the contractor will protect critical information including FOUO, PII, CPI and proprietary. The contractor OPSEC plan will be submitted to the 45 SW OPSEC SM within 90 days of contract award.
3. Contractors shall provide training to all employees within 90 days of hiring/assignment to a contract. Subcontractors should follow same guidance for protecting critical

information as outlined in the OPSEC plan. Training documentation should be provided to the unit OPSEC coordinator or OPSEC SM annually or as requested.
4. OPSEC training will be incorporated into annual security training.
5. The 45 SW will provide the contractor with information on developing an OPSEC plan. The 45 SW will also provide a Critical Information List (CIIL), basic threat information, OPSEC guidance and specific countermeasures.

2.2 DoD Common Access Card (CAC)

Access to certain facilities and the computer network requires a CAC. The issuance of CACs will be at Government expense. Access to classified or restricted areas may include additional requirements. Contractor shall maintain familiarity with local procedures for allowing access to work site and comply with all access requirements. CAC cards must be returned upon completion of the contract or earlier if the need has dissipated, for example, through termination of any employee. The capability of a potential employee being allowed access should be considered in all hiring and subcontracting decisions. The AF will not be responsible or liable for a Contractor's employee being denied issue of a CAC or access. These requirements may in some respect be in addition to those identified in AF Federal Acquisition Regulation Supplement (AFFARS) 5352.242-9000 Contractor Access to AF Installations and they also will be subject to the withholding provision.

3. Requirement/Description of Services

3.1 Develop and Provide RMF Artifacts for CDD-ER Systems

The contractor shall develop and provide relevant and accurate artifacts in support of the CDD-ER's acquisition of cybersecurity approval including, but not limited to, SCNs, ATCs, IATTs, and ATOs. The ISSE shall ensure the use of the most current government provided RMF templates of the cybersecurity process.

3.1.1 Topology

Contractor shall produce a Topology diagram that depicts the physical or logical configuration and authorization boundaries of each system.

3.1.2 Hardware and Software List

Contractor shall produce the Hardware and Software list for the system utilizing the most current template that can be exported and imported from eMASS (Enterprise Mission Assurance Support Service).

3.1.3 Ports, Protocols, and Services

Contractor shall produce Ports, Protocols, and Services Management (PPSM) for the system utilizing the most current worksheet from the AF PPS office.

3.2 Provide RMF Subject Matter Expertise

Using the ISSE's cybersecurity expertise, offer relevant recommendations for the implementation, immediate and planned, of STIGs and mitigations of risk in developing and supporting CDD-ER systems.

3.2.1 Plan of Action and Milestones (POA&M)

Contractor shall provide relevant input to the development of the POA&M.

3.2.2 STIG Applicability
Contractor shall produce STIG Applicability List for the system.

3.2.3 Documentation of Findings
The contractor shall document all findings and decisions for each applicable RMF control.

3.2.4 IPT Participation
The contractor shall attend 45th Space Wing integrated project team (IPT) meetings and provide expertise in support of the selection of cybersecurity controls for the Security Plan.

3.3 Compliance and Vulnerability Scans

3.3.1 Conduct the Execution of Vulnerability and Compliance Scanning
The contractor shall perform the necessary scans of CDD-ER systems using the most current, official criteria for inclusion in the RMF packages and in support of the development of the POA&M.

3.3.2 Compliance and Vulnerability Scan Reporting
Contractor shall produce the compliance and vulnerability scan results for all components of the system relevant to the accreditation or security change.

3.4 Participate in Security Test and Evaluations (ST&E) and Assessment Events
The contractor shall attend ST&E and assessment events to verify system security and configuration baselines. Baseline verification will require coordination with the project teams to coordinate test events during system implementation, or once the baseline has been defined. Test events will verify the hardware/software baseline, patch management, and configuration of the Defense Information Systems Agency (DISA) STIG. After each test event, the contractor team shall provide results to validate the accuracy of the baseline or will provide documentation to demonstrate discrepancies in the baseline to determine a fix action (e.g., System Security Baseline Report).

4. Contractual Requirements

4.1 Program Management
The ISSE shall also act as a Program Manager who shall be the primary representative responsible for all work awarded under this contract, participating in Program Management Reviews and ensuring all standards referenced herein are adhered to.

4.1.1 Reviews
The contractor shall conduct technical reviews for each assigned project in support of this task order. All reviews shall be held at the government facility or by teleconference. The contractor shall tailor all reviews for the unique aspects of this program. The following meetings are projected:

MEETING	LOCATION	Est. SCHEDULE
Kickoff	PAFB, CCAFS or telecom to be determined by Government	1 Week after award
Technical Interchange Meeting	PAFB, CCAFS or telecom to be	1 week after completion of system

	determined by Government	Security Plan 1st draft (90%)
Project Closeout Review	PAFB, CCAFS or telecom to be determined by Government	1 week after formal package submission to the government
Weekly Status Mtg	PAFB, CCAFS or telecom to be determined by Government	Weekly

4.1.2 Kickoff
The contractor shall schedule and facilitate a technical development team/Government kickoff meeting within one week of award to review and clarify, as required, technical requirements listed in section 3.0. This meeting must also identify contractor and Government points of contact, to include names, email addresses, and phone numbers.

4.1.3 Technical Interchange Meeting
Within one week following completion of a system Security Plan 1st draft, the contractor shall further collect, develop, and analyze project requirements and schedule and facilitate a Technical Requirements Review meeting with the contractor and Government. This meeting will detail the final agreed-upon requirements, clarifying any questions/concerns discussed during the kickoff meeting. During this meeting a project schedule will be negotiated between the contractor and government.

4.1.4 Project Closeout Review
Within 1 week of formal package submission to the government, the contractor shall schedule and facilitate a project closeout meeting. This meeting will summarize the work completed, and will identify best practices, as well as areas for improvement.

4.1.5 Weekly Status Meeting
During project execution, the contractor shall participate in weekly status meetings in order to gauge progress of assigned tasks.

4.1.2 Delivery of Services

4.1.2.1 Services Delivery Summary
The Services Delivery Summary (SDS) will be in accordance with AFI 63-101, Acquisition and Sustainment Life Cycle Management and FAR Subpart 37.6, Performance-Based Acquisition. SLAs will be defined in each TO.

Desired Outcome		**Performance Objective**	**Performance Threshold**	
Overall Outcome	Specific Outcomes		Target	Tolerance
RMF Artifacts	Ensure compliance with DoD and Air Force directives,	Deliver the Documents, Drawings, Diagrams, Spreadsheets,	Documentation submitted on schedule as defined in the government	90% of the time

	policies, guidance, and instructions	Checklists, etc. in compliance with RMF regulations and on time	approved project schedule.	
RMF Vulnerability and Compliance Results	Ensure compliance with DoD and Air Force directives, policies, guidance, and instructions	Deliver the Checklists, Spreadsheets, Scan Reports, STIGviewer, Vulnerator Reports, Cybersecurity Strategy, System Security Acquisition in eMASS. in compliance with RMF regulations and on time	Documentation submitted on schedule as defined in the government approved project schedule.	90% of the time
Presentation Materials	Provide program status to the government as required	Site Visit In-Briefs, Out-Briefs	Documentation submitted NLT 3 business days post presentation.	98% of the time
Monthly Accreditation status report	Provide and document monthly status of assigned programs	Deliver written status report	Delivered NLT 1 week after month end	98% of the time

4.1.2.2 Services Delivery Requirements

4.1.2.2.1 Release of Information

The contractor shall not release any information to any person, Government agency, or contractor concerning the program under this task order unless the procedures set forth in DFARS 204-7000, Disclosure of Information are followed.

4.1.2.2.2 Delivery Method

All data shall be delivered to the government technical lead via CDD Share Drive whenever possible. In cases where the data cannot be delivered via CDD Share Drive, email, AMRDEC Safe Access File Exchange (SAFE), or eMASS will be used.

4.1.2.2.3 Delivery Format and Frequency

The contractor shall deliver RMF artifacts as they are produced, in the format prescribed by the RMF templates, as applicable

4.1.2.2.4 Report Formats

Prescribed reports shall be delivered in a format approved by the government and must allow editing capability by the government (not .pdf).

4.1.3 TO Management

The contractor shall establish and provide a qualified workforce capable of performing the required tasks. The contractor shall use key performance parameters to monitor work performance, measure results, ensure delivery of contracted product deliverables and services, support management and decision-making and facilitate communications. The contractor shall identify risks, resolve problems and verify effectiveness of corrective actions. The contractor shall institute and maintain a process that ensures problems and action items discussed with the government are tracked through resolution and shall provide timely status reporting, via monthly accreditation status review meetings. Results of contractor actions taken to improve performance should be tracked and lessons learned incorporated into applicable processes. The contractor shall establish and maintain a documented set of disciplined, mature and continuously improving processes for administering all contract and TO efforts with an emphasis on cost-efficiency, schedule, performance, responsiveness and consistently high-quality delivery.

4.1.4 Configuration and Data Management

The contractor shall maintain and administer the government established 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, all RMF Artifacts, RMF Vulnerability and Compliance Results, and Presentation Materials The contractor shall provide the government with electronic access to this data, including access to printable reports.

4.1.5 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 PWS, 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 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 PWS or the NetOps and Infrastructure Solutions contract of which this PWS is a part (including all clauses that are or shall be included or incorporated by reference into that contract).

4.2 Security Management

4.2.1 Safeguarding Classified Information

The contractor shall transmit and deliver classified material/reports IAW the National Industrial Security Program Operations Manual (NISPOM) and the National Industrial Security Program Operating Manual (DoD 5220.22-M). These requirements shall be accomplished as specified in the TO. All Classified Contracts must have at a minimum, the Clause 52.204-2 Security Requirement, incorporated into the contract.

Each base will follow its own classified process IAW with the proscribed Federal guidance of the NISPOM and FAR “Subpart 4.4 along with DD Form 254. When transmitting classified

information ensure all classified information is properly sanitized and/or degaussed of all sensitive/classified information IAW AFSSI 5020.

For assistance and guidance on submitting Classified TO, the NETCENTS-2 Customer Service can be reached at COMM 334-416-5070 / DSN 312-596-5070 Option 1.

4.2.2 Personnel Security

The minimum level of security clearance to work on this task order is SECRET. Contractor shall ensure that ISSE personnel performing cybersecurity work are certified IAW DoDD 8140.01, and DoD 8570.01M.

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. In accordance with 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).

4.2.3 Protection of System Data

Unless otherwise stated in the TO, the contractor shall protect system design-related documents and operational data whether in written form or in electronic form via a network in accordance with 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 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.

4.2.4 Other Direct Cost (ODC)

The contractor shall identify ODC and miscellaneous items as specified in each TO. No profit or fee will be added; however, DCAA approved burdened rates are authorized.

4.2.5 Cyber Security Certification

Contractor shall ensure that ISSE personnel performing cybersecurity work are certified IAW DoDD 8140.01, DoD 8570.01M.

4.3 Government Furnished Items

4.3.1 Government Furnished Facilities

Contractor personnel working in a Government facility will be provided working space, communications equipment, network access, and general office supplies (e.g. paper, pens, pencils, paper clips) consistent with contract requirements. Work shall be performed in Government provided facilities at PAFB and CCAFS. The Government will provide workstations for all personnel. Workstations will include desk space, chairs, telephones, lighting, computers connected to Non-Secure Internet Protocol Network (NIPRNET), and use of community printers and fax machines.

4.3.2 Government Furnished Equipment
None

4.3.3 Government Furnished Material
None

4.3.4 Government Furnished Information
The government will provide:

- AFSPC RMF artifact templates
- System technical information
- System project schedule

4.3.2 Government Resources and Services
The government will provide:

1. Site access
2. System/enclave expertise and information
3. Sponsorship to the contractor for access to required information systems

5. Quality Processes

As a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the SEI SCAMPI, a method by an SEI-authorized lead appraiser, or comparable documented systems engineering processes, for the entire performance period of the contract, inclusive of options. Formal certifications must be held at the prime offeror's organizational level performing the contract. If not ISO certified or SEI appraised, acceptable comparable System Engineering processes shall be maintained for the entire performance period of the contract, inclusive of options. These processes include: requirements management; configuration management; development of specifications; definition and illustration of architectures and interfaces; design; test and evaluation/verification and validation; deployment and maintenance. The government reserves the right to audit and/or request proof of these comparable quality processes for the entire performance period of the contract, inclusive of options.

In addition, small business companion contract awardees that elect to take advantage of provisions outlined in clause H139 must comply with the quality processes requirements. This means that at the time of award and as a minimum, the prime contractor shall be appraised at ISO 9001:2000 or ISO 9001:2008 or ISO/IEC 20000 or CMMI Development Level 2 (or higher) using the Software Engineering Institute's (SEI) SCAMPI A method by an SEI-authorized lead appraiser and must be held at the prime offeror's organizational level performing the contract for the entire performance period of the contract, inclusive of options. Evidence of comparable Systems Engineering (SE) processes will not be accepted.

Appendix 1: NetOps and Infrastructure Solutions Standards & References

Purpose:

The following certifications, specifications, standards, policies and procedures in Table 2 represent documents and standards that may be placed on individual contract task orders. Individual task orders may impose additional standards to those required at the contract level. The list below is not all-inclusive and the most current version of the document in the AF Standard Center of Excellence Repository (SCOER) at the time of task order issuance will take precedence. Other documents required for execution of tasks issued under NETCENTS-2 will be cited in the relevant Task Order, such as specific FIPS, NIST, or MIL-Standards.

DOCUMENT	TITLE	DATE
AFI 10-701	Operations Security (OPSEC)	8 June 2011
AFI 63-101	Integrated Life Cycle Management	9 May 2017
AFI 33-364	Records Disposition—Procedures and Responsibilities	22 December 2006
AFMAN 33-363	Management of Records	1 March 2008
CNSSI 1253*	Security Categorization and Control Selection for National Security Systems	27 March 2014
AFSPCI 33-202	Administrative Procedures	7 May 2014
FISMA	Federal Information Security Management Act	18 December 2014
DoDI 5000.02	Operation of the Defense Acquisition System	7 January 2015
DoDI 8500.01	Cybersecurity	14 March 2014
DoDD 8140.01	Cyberspace Workforce Management	11 August 2016
DoDD 8570.01M	Information Assurance Workforce Improvement Program	10 November 2015
DoDD 5205.02E	DoD Operations Security (OPSEC) Program	20 June 2012

DoDI 8510.01	Risk Management Framework for DoD IT	12 March 2014
FIPS Pub 199	Federal Information Processing Standards Publication 199 Standards for Security Categorization of Federal Information and Information Systems	February 2004
Special Publication 800-37, Revision 1	National Institute of Standards and Technology (NIST) Guide for Applying the Risk Management Framework to Federal Information System	February 2010
Special Publication 800-53, Revision 5	National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems and Organizations	April 2013
Special Publication 800-53A	National Institute of Standards and Technology (NIST) Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans	December 2014
Special Publication 800-60, Revision 1	National Institute of Standards and Technology (NIST) Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes 1 and 2	August 2008
STIG Viewer 2.0 User Guide	STIG Viewer to be used to select the appropriate Defense Information Systems Agency (DISA) Security Technical Implementation Guides	December 2015

Attachment 1 – Contract Deliverables

The Government requires all deliverables that include Scientific and Technical Information (STINFO), as determined by the Government, be properly marked IAW DoDI 5230.24 and AFI 61-204 prior to initial coordination or final delivery. Failure to mark deliverables as instructed by the government will result in non-compliance and non-acceptance of the deliverable. The contractor will include the proper markings on any deliverable deemed STINFO regardless of media type, stage of completeness or method of distribution. Therefore, even draft documents containing STINFO and STINFO sent via e-mail require correct markings. Additionally, as required by individual Task Orders, the contractor shall formally deliver as a CDRL all intellectual property, software, licensing, physical records, files, documents, working papers and other data for which the Government shall treat as deliverable.

Table A1.1 contains the applicable CDRLs for this contract effort.

CDRL	Title
A038	Information Systems Accreditation Documentation
A062	Status Report
A087	Technical Report - Study/Services
A112	Engineering Drawings
A149	Security Vulnerability Analysis
A166	OPSEC Plan
A120	Certification/Data Report
A212	Functional Flow Diagram
A301	Briefing Material
A381	Information Assurance (IA) Test Report
A382	Information Assurance (IA) Test Plan
A383	Information Assurance (IA) Design Review Information Package (DRIP)

Table A1.1 CDRLs

The corresponding deliverable is identified in the test below with the CDRL is parenthesis. CDRL deliverables will be tailored to fit cybersecurity efforts during the kickoff meeting.

Program Management Deliverables

- OPSEC Plan (A166)
- Site Visit in-briefs (A301)
- Out-briefs (A301)
- Monthly Status Reports (A062)
- Other administrative documentation

Technical Deliverables

Cybersecurity Test Report (A381)

Cybersecurity Test Plan (A382)

RMF Artifacts (A038, A087, A149, A120, A383) including, but not limited to:

- As-built topology (A112, A212)
- Hardware list (A038)
- Software list (A038)
- Ports, protocols and services worksheet (A038, A149)
- Initial, baseline configuration files of device/software/system (A038)
- Configuration management plan (A038,A149)
- System categorization memo (A038, A149)
- Organization risk tolerance balance (ORTB) artifacts and follow-on artifacts (A038, A149)
- Security and contingency plan (A038, A149)
- Other documents, drawings, diagrams, spreadsheets, and checklists in compliance with RMF regulations (A038,A149)

RMF Vulnerability and Compliance Results (A038, A087, A149, A120, A383) including, but not limited to:

- Checklists (A038,A149)
- Spreadsheets (A038,A149)
- Scan Reports (A038,A149)
- STIGviewer (A038,A149,A383)
- Vulnerator Reports (A038,A149, A383)
- Cybersecurity Strategy (A038,A149)
- System Security Acquisition (A038,A149)

Attachment 2 – Workload Factors

1. Workload Summary

Work to be performed is project centric and is not expected to be constant over the course of the period of performance. Workload estimates for the period of performance are shown in Table A2.1

Work type	Total hours estimated for PoP
Program Management	76 hours
RMF Artifacts	621 hours
RMF Vulnerability and Compliance Results	267 hours
Total	960 hours

Table A2.1 Total man hour estimates

2. Workload Breakdown

Program Management

4 weekly meetings/month each estimated to be 1 hour in length

1 monthly status report, each estimated to require 1.5 hours to complete

1 presentation every 2 months, each estimated to require 1.5 hours to complete

RMF Artifacts

RMF Artifacts for 3 separate projects, each estimated to require 207 hours to complete

RMF Vulnerability and Compliance Results

RMF Vulnerability and Compliance Results for 3 separate projects, each estimated to require 89 hours to complete