Volume II – Technical

Cybersecurity Risk Management Framework Support IDIQ

Department of the Air Force

Solicitation# FA7037-15-R-0009

Due Date: December 09, 2015 at 12:00 PM CST

Prepared for and Presented to:

Attention: Teresa J. Gonzalez
Department of the Air Force
102 Hall Blvd, Ste 258
Lackland AFB, Texas 78243
Phone: 210-977-6095
Email: teresa.gonzalez@us.af.mil

Prepared and Presented by:

Insert your company information here

Insert Your Company Logo Here

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of or in connection with the submission of this data, the Government shall have the right to duplicate, use or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained on the pages marked with the legend "Use or disclosures of data contained on this sheet is subject to the restriction on the title page of this proposal."

Transmittal Letter

December 09, 2015

Submission Method: Paper Copy and CD-ROMs Submission

Department of the Air Force
102 Hall Blvd, Ste 258
Lackland AFB, Texas 78243

Attention: Ms. Teresa J. Gonzalez

Subject: Response to Combined Synopsis/Solicitation FA7037-15-R-0009 – Cybersecurity Risk Management Framework Support IDIQ.

Dear Ms. Gonzalez:

Sincerely,

/Signature/

Authorized Person

Table of Contents

List of Table and Drawings

Glossary of Acronyms and Abbreviations (No Page Limit)

Acronym/Abbreviation	Explanation

VOLUME II – TECHNICAL (35 PAGE LIMIT) [INSTRUCTION TO OFFEROR (ITO).5.0, EVALUATION (EVAL) B.3.0]

5.1 General – Ensure Technical volume is specific and complete. Legibility, clarity, and coherence are very important. Your responses will be evaluated against the Technical subfactors defined in 52.212-2, Evaluation -- Commercial Items. Using the instructions provided below, provide as specifically as possible to the actual methodology you would use for accomplishing/satisfying these subfactors. All the requirements specified in the solicitation are mandatory. By your proposal submission, you are representing that your firm will perform all the requirements specified in the solicitation. It is not necessary or desirable for you to tell us so in your proposal. Do not merely reiterate the objectives or reformulate the requirements specified in the solicitation. The proposal shall provide a descriptive narrative with convincing rationale to address how the offeror intends to meet the requirements of the solicitation.

5.1.3 Technical volume will be the primary basis for evaluating your proposed approach to meeting or exceeding the minimum performance or capability requirements of each technical subfactors. Your proposal shall describe the capability of your organization to perform this contract including pertinent aspects of the proposed approach such as teaming or subcontracting arrangements.

1 SUBFACTOR 1: CYBERSECURITY RISK MANAGEMENT FRAMEWORK STRATEGY [ITO 5.2, EVAL B.3.1]

5.2 Technical Subfactor 1: Cybersecurity Risk Management Framework Strategy (Most Important under Technical)

Under this subfactor discuss your technical understanding of Cybersecurity Risk Management Framework operations, to include the following:

***Introductory heading. Actual response should be detailed in sub paragraph below. ***

1.1 Cybersecurity Risk Management Framework [ITO 5.2.1, Eval B.3.1.1]

5.2.1 Describe your experience, approach, and techniques utilized for identifying, evaluating and integrating security controls as it relates to Cybersecurity Risk Management Framework. Include your experience with the Intelligence Community to include policy development in both content and format.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

1.2 Security Coordination Center and Incident Response Center Service Provider [ITO 5.2.2, Eval B.3.1.2]

5.2.2 Describe your approach to Security Coordination Center and Computer Network Defense Service Provider (CND-SP) operations to include reviewing, developing, and implementing test and evaluation events for vulnerability management and reporting. Include your experience with threat-based signature development, forensic analysis, enterprise/near-real time mapping and network tools for Government Intrusion Detection/Prevention Systems.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

1.3 Information Systems Security Training & ICD 502 and ICD 503 [ITO 5.2.3, Eval B.3.1.3]

5.2.3 Describe your experience, capabilities and approach in developing and delivering information systems security training encompassing the concepts of the National Institute of Standards and Technology (NIST) Risk Management Framework and intelligence community requirements under ICD 502 and ICD 503.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

1.4 Air Force Software Certification [ITO 5.2.4 Eval B.3.1.4]

5.2.4 Describe your capabilities and approach to conducting technical evaluation attributes for the AF software certification program as well as your abilities and approach to manage an on-line presence including web and SharePoint content on multiple networks. Technical evaluation includes the ability to read and understand software vulnerability reports in order to make certificate to field recommendations.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

1.5 Systems Engineering [ITO 5.2.5, Eval B.3.1.5]

5.2.5 Describe in a plan how you will manage systems engineering to include modernization leading to the integration, test, installation, evaluation and training for sustainment and enhancement of existing system security technologies, including but not limited to commercial of the shelf (COTS)/ Government off the shelf (GOTS).

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

2 SUBFACTOR 2: STAFFING STRATEGY [ITO 5.3, EVAL B.3.2]

5.3 Technical Subfactor 2: Staffing Strategy

Under this subfactor, contractors must demonstrate a well-developed, comprehensive strategy to integrate personnel throughout the various mission sets with minimal disruption at contract kick-off and throughout the life of the contract. It should also include training/certification consideration required to ensure employees maintain necessary certification levels required by the contract.

***Introductory heading. Actual response should be detailed in sub paragraph below. ***

2.1 DoD 8570.01M [ITO 5.3.1, Eval B.3.2.1]

5.3.1 Develop a comprehensive staffing plan that describes your team member staffing process and approach to integrating new personnel to the project. Detail shall include training plans to maintain personnel certifications required by DoD 8570.01M as outlined in PWS Appendix B

throughout the life of the contract. For each labor category, provide documentation demonstrating your ability to provide personnel with the required certifications, education, and years of experience as required by DoD 8570.01M Certification. 100% compliance is required on day-one of the Period of Performance.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

2.1.1 Team Member Staffing Process and Approach to Integrating New Personnel to the Project

Start typing your response here…

2.1.2 Training Plans to Maintain Personnel Certifications

Start typing your response here…

2.1.3 Ability to Provide Personnel with the Qualification and Required Certifications

Start typing your response here…

2.2 Team Structure Matrix [ITO 5.3.2, Eval B.3.2.2]

5.3.2 Include a Team Structure Matrix for your company and all subcontractors, teaming partners, and/or joint venture partners who are proposed to perform 10 percent or more of the proposed effort based on the total proposed price or perform aspects of the effort the offeror considers critical to overall successful performance. The Team Structure Matrix shall identify all the proposed work and PWS requirements the offeror, subcontractor, teaming partners, and/or joint venture partners will perform and what percentage of the proposed effort they will perform.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

2.3 Customer Service [ITO 5.3.3, Eval B.3.2.3]

5.3.3 Describe your management approach for providing timely, accurate and responsive customer service. This approach should include the potential capability for 24/7 support (as during flexed operations).

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

2.4 Security Clearance Management [ITO 5.3.4, Eval B.3.2.4]

5.3.4 Describe your ability to provide personnel that can satisfy the Contract Security Specifications established in DD Form 254 at time of award. Identify and describe your staffing plan for ensuring 90% of employees have the necessary TS/SCI w/SB clearances on day one of

the period of performance and 100% by day 31. Include a management plan to ensure all employees maintain the appropriate security clearances to conduct operations throughout the life of the contract.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

2.4.1 Staffing Plan to Identify TS/SCI w/SB Cleared Employees

Start typing your response here…

2.4.2 Management Plan to Maintain Appropriate Security Clearances of Employees

Start typing your response here…

3 SUBFACTOR 3: MANAGEMENT APPROACH [ITO 5.4, EVAL B.3.3]

5.4. Technical Subfactor 3: Management Approach–Define in detail your management approach to include the following:

***Introductory heading. Actual response should be detailed in sub paragraph below. ***

3.1 Personnel Retention Methods & IDIQ Personnel Management [ITO 5.4.1, Eval B.3.3.1]

5.4.1 Provide a plan that addresses your acquisition and retention methods for skilled and certified personnel, including retention during times of limited taskings. Demonstrate how you will manage the Cybersecurity Risk Management Framework IDIQ contract to include multiple task orders at various geographical locations where ISR is conducted.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

3.2 Personnel Management Plan [ITO 5.4.2, Eval B.3.3.2]

5.4.2 Describe your plan to manage personnel during various shift schedules, including accountability of personnel, and that subcontractors utilized on the contract are properly managed and that information is appropriately disseminated. In your plan describe how you will manage personnel resources across multiple projects. Include in your plan tracking project progress from initial tasking through completion.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

3.2.1 Subcontractor Management

Start typing your response here…

3.2.2 Managing Personnel Resources Across Multiple Projects

Start typing your response here…

3.2.3 Tracking Project Progress from Initial Tasking through Completion

Start typing your response here…

3.3 Intellectual Property Management [ITO 5.4.3, Eval B.3.3.3]

5.4.3 Provide a plan for the development, implementation and management of the creation of intellectual property. Include how you will ensure your plan's effectiveness and maintain continuity for future Government capability.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4 SUBFACTOR 4: ACC/A2S-OL AND 25 AF ISR RMF TASK ORDER 0001 [ITO 5.5, EVAL B.3.4]

5.5 Technical Subfactor 4: ACC/A2S-OL and 25 AF Risk Management Framework Task Order 0001: This Task Order 0001 will be executed as the first task order against the basic contract.

***Introductory heading. Actual response should be detailed in sub paragraph below. ***

4.1 Proposal Strategy to include Labor Mix [ITO 5.5.1, Eval B.3.4.1, PWS 2.0]

5.5.1 Describe your strategy for ensuring that all requirements are met IAW the Performance Work Statement for Task Order 0001, Attachment #2. Describe the Labor Categories and number of Labor Hours proposed to meet this requirement, the total price/cost will be calculated using the fully loaded labor rates (Attachment #3).

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2 Technical Approach (PWS – Task Order 0001) [ITO 5.5.2, Eval B.3.4.2]

5.5.2 Provide a management plan on how you will incorporate subfactors one (1), two (2) and three (3) as it applies to Task Order 0001 only. Include your strategy for insuring that all requirements are met under the task order beginning at task order award. The strategy shall include the approach assuring full support for the work (PWS Attachment #2) defined for Task Order 0001 for the entire period of performance.

2.0 SPECIFIC TASKS.

The contractor shall provide the following cybersecurity tasks in support of the AF IC CIEO, CISO, AO and REM requirement to manage risk and protect the confidentiality, integrity, availability of our AF IC missions and resources.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.1 Program Management for Implementing AF IC Enterprise Cybersecurity Solutions [PWS 2.1]

The contractor shall serve as a program manager to implement AF IC Enterprise-wide cybersecurity solutions for the AF IC CISO, AF IC AO, AF IC REM. The contractor shall adhere to AF and IC standards and those processes as further defined by the Government Subject Matter Expert (SME). The contractor shall conduct timely and in-depth research for policies and processes. The contractor shall provide recommendations to the Government SME by defined deadlines. Recommendations shall include test plans and procedures to ensure results support the required objectives and capabilities. The contractor shall apply IT security control requirements to address thelevelofsecurityrequiredtoprotecttheconfidentiality,integrityandavailabilityofthe system data and resources. Solutions shall be compatible with system or network hardware and software configurations and shall be approved by the configuration managers of the system and network. The contractor shall assess the “as is” and provide a “to be” for various projects. The contractor shall interact with various ISR program offices to plan and implement cybersecurity solutions throughout the enterprise. The contractor shall utilize effective communication skills to interact and push implementations to Government SME. The contractor shall use the RMF methodology to successfully implement an information technology process which shall effectively protect the element's information assets and its ability to perform its mission. The contractor shall participateinmeetingsandprogramreviewstosupporttheimplementationof ISR initiatives, goals and objectives. The contractor shall provide the AF IC CISO with the operational and economic costs of protective measures so they may be weighed against requirements for mission accomplishment. The contractor shall make edits to existing Government documents, prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of assigned task. The contractor shall test alternatives and provide test results to the Government for decision-making. The contractor shall review Government documents and provide their comments in required formats. The contractor shall provide on-the-job training to military, civilians and contractors concerning the new procedures for their specific project. This is not formal training, but informal office training. Provide weekly status updates through the contractor lead for quality control and consolidation into one (1) weekly activity report to be provided to the COR. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. If required to implement a cybersecurity initiative, the PM shall complete the Assessments and Authorizations (A&A) documents required to obtain an ATO. The contractor shall complete POA&Ms for the project to address security vulnerabilities. The contractor shall complete trip reports for each trip taken and complete meeting minutes. (A001.A002, A003, A004, A005, A006, A007, A008, A009, A011, A013)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.2 IT Security Control Assessments [PWS 2.2]

2.2.1 The contractor shall serve as a security control assessor (SCA). A SCA shall meet the minimum qualification requirements as identified by AF and IC security control assessment polices (in accordance with PWS attachment Appendix B). The SCA shall complete required reports for a risk decision from the AO or CISO. The contractor shall adhere to USAF and IC laws, standards, policies and procedures. The contractor shall conduct comprehensive IT security control assessments on systems identified within the scope of this contract. Assessments shall require physical travel to various contractor and Government sites inside and outside the continental United States (CONUS and OCONUS). Assessments shall determine the condition of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). The contractor shall provide an assessment on the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive (A013).

2.2.2 The contractor shall review the System Security Plan (SSP), prior to initiating the security control assessment and ensure the plan provides a set of security controls for the information system that meet the stated security requirements. Assessments shall include the review and validation of the message types authorized and the parsing of the data utilizing rule sets implemented within the Cross Domain Solutions (CDS) application to validate authorized processing of data and elimination of the possible spillage of classified information.

2.2.3 The contractor shall:

2.2.3.1 Advise the Information System Owner (ISO) concerning the impact values for confidentiality, integrity, and availability for the information on a system;

2.2.3.2 Evaluate threats and vulnerabilities to information systems to ascertain the need for additional safeguards;

2.2.3.3 Review and approve the information system security assessment plan, which is comprised of the SSP, the Security Controls Traceability Matrix (SCTM), and the Security Control Assessment Procedures;

2.2.3.4 Ensure security control assessments are completed for each information system and ensure controls are working as intended and these controls protect the confidentiality, integrity and availability of IT resources at the appropriate levels;

2.2.3.5 Prepare the final Security Assessment Report (SAR) containing the results and findings from the assessment at the conclusion of each security control assessment activity; (A013)

2.2.3.6 For each completed trip provide a trip report; (A011)

2.2.3.7 Ensure a Plan of Action and Milestones (POA&M) is initiated by the ISSO for the information system based on findings and recommendations from the SAR; (A007)

2.2.3.8 Evaluate security control assessment documentation and provide written recommendations for security authorization to the AO; (A013)

2.2.3.9 Assemble and submit the security authorization artifacts to the AO (consisting of, at a minimum, the SSP, the SAR, the POA&M, and a Risk Assessment Report (RAR); (A007, A011, A013)

2.2.3.10 Assess the proposed changes to information systems, their environment of operation, and mission needs to determine if they are security-relevant and could therefore affect system authorization;

2.2.3.11 Use AF IC Security controls defined by the AO and CISO;

2.2.3.12 Utilize the RMF methodology to successfully implement an information technology process which shall effectively protect the element's information assets and its ability to perform its mission;

2.2.3.13 Submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR; (A003)

2.2.3.14 Provide guidance to other assessors on the policies and procedures of the job;

2.2.3.15 Provide detailed assessment findings using Government-specified processes and procedures;

2.2.3.16 Provide solutions and recommendations to remedy security vulnerabilities, threats, to ultimately improve the protection of IT resources and to execute the AF ISR mission; (A006, A013)

2.2.3.17 Utilize assessment results to identify trends and to improve IA training, policies and processes.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.3 Cybersecurity Engineering [PWS 2.3]

The contractor shall serve as the security engineer and provide the Government SME with recommendations and solutions for implementing AF IC cybersecurity programs and projects. The contractor shall adhere to AF and IC standards and those processes as further defined by the Government SME. The contractor shall provide program reviews, schedules, action item updates and required procedures by established deadlines. The contractor shall conduct timely and in-depth research for policies and processes. The contractor shall apply IT security control requirements to address the level of security required to protect the confidentiality, integrity and availability of system data and resources. Solutions shall be compatible with system or network hardware and software configurations and shall be approved by the configuration managers of the system and network. Recommendations shall include test plans and procedures to ensure results support the required objectives and capabilities. The contractor shall assess the “as is” and provide a “to be” for various projects. The contractor shall use the RMF methodology to successfully implement an information technology process, which shall effectively protect the element's information assets and its ability to perform its mission. The contractor shall perform Security, Test and Evaluation (ST&E) for each system prior to the assessment phase for each

system. The contractor shall perform scans of systems and architectures using AF IC -approved scanning tools during the ST&E event. The contractor shall construct and provide ST&E reports that contain the scans, Security Technical Implementation Guide (STIG) application with issues and recommendations for delivery prior to the assessment event. The contractor shall perform software security analysis and review to include software source, commercial-off-the-shelf (COTS) compatibility, original equipment manufacturer (OEM) source, source code availability and impact to system integration and operations. The contractor shall execute all applicable Supply Chain Risk Management (SCRM) policy and procedure and create reports for all new additions of system hardware and software to determine the source from the OEM through the end supplier to ensure SCRM is followed per policy and guidelines. The contractor shall complete reports, plans and procedures. The contractor shall participate in meetings and program reviews and support the implementation of ISR initiatives, goals and objectives. The contractor shall provide the AF IC CISO with the technical costs of protective measures so they may be weighed against requirements for mission accomplishment. The contractor shall make edits to existing Government documents, prepare briefings as required to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. If required to implement a cybersecurity initiative, the PM shall complete the A&A documents required to obtain an ATO. The contractor shall complete POA&Ms for the project to address security vulnerabilities. The contractor shall complete trip reports for each trip taken and provide weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR.

The contractor shall complete and provide meeting minutes to the COR. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. (A001, A002, A003, A004, A005, A006, A007, A008, A009, A011, A013)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.4 Plans, Policies, and Procedures [PWS 2.4]

The contractor shall develop and provide well-defined plans, policies, agreements and procedure recommendations on how to effectively maintain IT security control requirements and successfully meet AF and IC cybersecurity mandates. The contractor shall professionally interact with managers and site personnel and present oral and written process solutions. The contractor shall review, edit, comment, analyze documents and recommend corrections and changes. The contractor shall use the RMF methodology to successfully implement an information technology process, which shall effectively protect the element's information assets and its ability to perform its mission. The contractor shall ensure risk management is integrated into the technical, physical and administrative controls throughout the network, system, database, and application lifecycle. Submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. The contractor shall develop and conduct technical or procedural training for military, civilian and contractor cybersecurity professionals on IA topics primarily using curriculum provided by the Government. This is not formal training, but informal office training. The contractor shall develop and provide on-the-job training to Government, contractor and military personnel on various IT security tools, policies and

procedures required to protect resources and meet standards only when tasked by the COR. The contractor shall complete trip reports for each trip taken and meeting minutes for Policy Team led meetings. The contractor shall make edits to existing Government documents, prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. (A001, A003, A006, A008, A009, A011)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.5 Content Management and Development [PWS 2.5]

The contractor shall expertly manage the AF IC cybersecurity collaborative environments for successful day-to-day business operations on networks at the UNCLASSIFIED, SECRET and TOP SECRET security levels. The contractor shall maintain SharePoint and websites so customers can access the cybersecurity information required of the AF IC CISO, AO and their SMEs. The contractor shall implement high quality, scalable, and extendable SharePoint solutions using the .NET Framework, ASP.net, SharePoint (currently using version 2013) and other advanced components of Microsoft technology. The contractor shall publish Access databases to SharePoint and develop custom forms using InfoPath. Expert knowledge of HTML and JavaScript are required to create custom web parts. The contractor shall utilize Microsoft SharePoint Designer to customize sites and create custom workflows. The contractor shall have a solid grasp of the permissions hierarchy of the SharePoint application. The contractor shall transform customer requirements into viable SharePoint- involved solutions. The contractor shall address possible solutions and timeframes for completion with the customer for each tasking. Once the solution is implemented, access to the site, library, or object shall be controlled through permissions provided by the particular Government SME. The contractor shall test all content management solutions followed by the end user before being deployed to production. The contractor shall field all SharePoint-related questions concerning the sites they manage including requests for site access. The contractor shall use the RMF methodology to successfully implement an information technology process, which shall effectively protect the element's information assets and its ability to perform its mission. The contractor shall ensure risk management is integrated into the technical, physical and administrative controls throughout the network, system, database, and application lifecycle. The contractor shall develop and provide detailed weekly status reports to address the status of tasks accomplished for the previous week’s activities. Submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. The contractor shall develop and provide on-the-job training to Government, contractor and military personnel on content management and procedures and processes only when tasked by the COR. This is not formal training, but informal office training. The contractor shall review and edit documents and recommend corrections and changes. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. The contractor shall make edits to existing Government documents, prepare briefings to update the

Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. (A003, A008, A009, A013)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.6 AF IC Security Coordination Center Support Services [PWS 2.6]

The contractor shall manage twenty-four (24) hour command and control (C2) services to the AF IC CISO and the REM and appointed Government SMEs for situational awareness, analysis and reporting on the integrated defense risk for SCI and ISR resources to ODNI, AF/A2 and AF/A6. Services shall include the research, development and release of AF IC Task Orders (TASKORDS) and notifications to the AF IC. The contractor shall comply with coordination processes and approvals, formats and reporting requirements as defined by the Government. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. The contractor shall complete trip reports for each trip taken and complete meeting minutes. The contractor shall complete reports, plans and. The contractor shall submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. When tasked by the COR, the contractor shall develop and provide on-the-job training to Government, contractor and military personnel on various IT security tools, policies and procedures required to protect resources and meet standards. This is not formal training, but informal office training. The contractor shall make edits to existing Government documents, prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. Provide situational reports to the AF IC CISO to ODNI and A2. (A001, A002, A003, A008, A009, A010, A011, A013)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.7 RESERVED [PWS 2.7]

Start typing your response here…

4.2.8 Cybersecurity Training [PWS 2.8]

The contractor shall conduct technical and managerial level training on information assurance, security tools and A&A work flow tools topics primarily using curriculum provided by the Government. The contractor shall develop additional technical and managerial IA training plans, guides, materials and curriculum to enable compliance with USAF, DoD, IC and other national agency standards. This training shall keep AF IC IT security professionals familiar with the various IT security tools, policies and procedures required to protect resources and meet standards. Training critiques shall be used to assess the instructor performance and update training materials. The contractor shall submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. The contractor shall complete trip reports for each trip taken. The contractor shall complete meeting minutes. The contractor shall make edits to existing Government documents, prepare briefings to update

the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. The contractor shall review and edit documents and recommend corrections and changes. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. (A001, A003, A008, A009, A011, A012)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.9 Document Management [PWS 2.9]

The contractor shall provide services for document management supporting the AF IC CISO and staff to gather information from SMEs in the completion of various documents and tasks. The contractor shall prepare, edit, and maintain policy documentation; maintain schedules; accountability of various tasks; develop and process records management; maintain the AF file plan; review and edit staff created documents prior to internal and external dissemination; facilitate and participate in AF IC- level cybersecurity policy discussions and working groups; research, develop, update, and distribute branch related communications; coordinate the publication and distribution of new and revised policies; maintain accurate records and historical changes of policies and procedures. The contractor shall complete meeting minutes. Performs as alternate Computer Support Liaison (formerly Information Assurance Officer) and submit request to provision/de-provision personnel and organizational network accounts and primary focal point for computer assistance. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. The contractor shall prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. The contractor shall submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. (A001, A003, A008, A009)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.10 Assessment and Authorization Support Analysis [PWS 2.10]

The contractor shall provide analytical and documentation support to the AF IC CISO SMEs in AF IC Risk Management. Duties shall include day-to-day support to the Delegated Authorizing Officials (DAOs) and the Security Control Assessments (SCAs) and shall include drafting and tracking Security Impact Analyses (SIAs) used in support of Continuous Monitoring; coordinating Discovery Meetings and ensuring updated Discovery Meeting checklists are uploaded into the A&A Workflow tool; drafting Interim Approvals to Test (IATTs) and Authorities to Operate (ATOs); uploading the IATTs and ATOs into the workflow tool once finalized; provide workflow tool support to site personnel; monitoring and reporting FISMA compliance and ensure ATO dates in the workflow tool match the dates in the official ATO MFRs; analyze RMF workflow tasks prior to Assessment to ensure all processes are filled out as required. Initiatives to support the SCAs include the review vulnerability scans and corresponding non- mitigation worksheet (this supports Continuous Monitoring requirements);

and the review of software, hardware, and PPS (ports, protocols, and services) against Approved Products List, Certificates to Field, and DISA Category Assurance Levels (CAL). The contractor shall complete meeting minutes as defined by the COR. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. The contractor shall make edits to existing Government documents, prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. The contractor shall complete trip reports for each trip taken and complete meeting minutes. The contractor shall submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. (A001, A002, A003, A008, A009, A011)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

4.2.11 Information Assurance Program Management Support Services [PWS 2.11]

The contractor shall perform IA support services to assist AF IC IA Program Managers and Information System Security Officers/Managers (ISSO/ISSMs) at Joint Base Langley, VA and Joint Base San Antonio, TX. The Contractor shall assist in maintaining an effective cybersecurity program that supports missions and adequately protects the confidentiality, integrity and availability of our AF IC information resources. The contractor shall gather data, analyze compliance and report results on the condition and progress of AF IC IA programs, security plans, plan of action and milestones (POA&M) and A&A workflow tools data, patch management, information assurance vulnerability alerts (IAVA), DoD 8570.01M certifications and FISMA compliance requirements, and ATOs. The contractor shall make edits to existing Government documents, prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. The contractor shall complete meeting minutes. The contractor shall interact with Unit ISSOs/ISSMs and commanders to provide IA guidance, complete IA assessment reports and provide solutions to commanders on how to improve their IA programs. The contractor shall submit weekly status updates through the contractor lead for quality control and consolidation into one (1) weekly activity report to be provided to the COR. The contractor shall develop and provide on-the-job training to Government, contractor and military personnel on various IT security tools, policies and procedures required to protect resources and meet standards. This is not formal training, but informal office training. Complete trip reports for each trip taken. The contractor shall support the Cybersecurity trainers with updated information and materials for their area of responsibility for compliance with USAF, DoD, IC and other national agency standards. The contractor shall complete reports, plans and procedures as defined by the COR. (A001, A003, A006, A008, A009, A011)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5 CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES (NO PAGE LIMIT)

Based on the Question No. 22, Continuation Of Essential Contractor Services – needs to be submitted as part of the Technical Volume. This plan is exempt from the total page count of Technical Volume.

252.237-7024 NOTICE OF CONTINUATION OF ESSENTIAL CONTRACTOR SERVICES (OCT 2010)

(a) Definitions. Essential contractor service and mission-essential functions have the meanings given in the clause at 252.237-7023, Continuation of Essential Contractor Services, in this solicitation.

(b) The offeror shall provide with its offer a written plan describing how it will continue to perform the essential contractor services listed in Attachment 1, paragraph 2.6, Mission Essential Contractor Services (AF IC Security Coordination Center Support), dated 17 Sep 2015, during periods of crisis. The offeror shall—

5.1 AF IC Security Coordination Center Support [PWS 2.6]

The contractor shall manage twenty-four (24) hour command and control (C2) services to the AF IC CISO and the REM and appointed Government SMEs for situational awareness, analysis and reporting on the integrated defense risk for SCI and ISR resources to ODNI, AF/A2 and AF/A6. Services shall include the research, development and release of AF IC Task Orders (TASKORDS) and notifications to the AF IC. The contractor shall comply with coordination processes and approvals, formats and reporting requirements as defined by the Government. The contractor shall create, maintain and dispose of only those Government required records and supporting documentation that are specifically cited in this Performance Work Statement (PWS) or required by the provisions of a mandatory directive. The contractor shall complete trip reports for each trip taken and complete meeting minutes. The contractor shall complete reports, plans and. The contractor shall submit weekly status updates through the contractor leads for consolidation into one (1) weekly activity report to be provided to the COR. When tasked by the COR, the contractor shall develop and provide on-the-job training to Government, contractor and military personnel on various IT security tools, policies and procedures required to protect resources and meet standards. This is not formal training, but informal office training. The contractor shall make edits to existing Government documents, prepare briefings to update the Government on the status of actions and coordinate with all project members to meet the goals and objectives of the assigned task. Provide situational reports to the AF IC CISO to ODNI and A2. (A001, A002, A003, A008, A009, A010, A011, A013)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5.1.1 Provisions for Acquisition of Essential Personnel and Resources

(1) Identify provisions made for the acquisition of essential personnel and resources, if necessary, for continuity of operations for up to 30 days or until normal operations can be resumed;

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5.1.2 Challenges Associated with Maintaining Essential Contractor Services

(2) Address in the plan, at a minimum--

(i) Challenges associated with maintaining essential contractor services during an extended event, such as a pandemic that occurs in repeated waves;

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5.1.3 Time Lapse Associated with the Initiation of the Acquisition of Essential Personnel and Resources

(ii) The time lapse associated with the initiation of the acquisition of essential personnel and resources and their actual availability on site;

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5.1.4 Components, Processes, and Requirements for the Identification, Training, and Preparedness of Personnel

(iii) The components, processes, and requirements for the identification, training, and preparedness of personnel who are capable of relocating to alternate facilities or performing work from home;

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5.1.5 Established Alert and Notification Procedures for Mobilizing Identified ``Essential Contractor Service'' Personnel

(iv) Any established alert and notification procedures for mobilizing identified ``essential contractor service'' personnel; and

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

5.1.6 Approach for Communicating Expectations to Contractor Employees

(v) The approach for communicating expectations to contractor employees regarding their roles and responsibilities during a crisis.

(End of provision)

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

6 CROSS REFERENCE MATRIX [ITO 6.0]

6.1. Offerors shall complete the Cross-Reference Matrix at Table B-2 and include in Volume II. The Cross- Reference Matrix provides critical interrelationships and dependencies between the PWS, Instructions to Offerors and Evaluation of Offers of the RFP, and the offeror's proposal. The Government has completed the Description, Instructions to Offerors and Evaluation of Offers Columns; the offerors shall complete "Proposal Volume, Section No., Page & Para No." column.

6.2 The purpose of the cross-reference matrix is to show critical interrelationships and dependencies among the technical requirements document PWS, 52.212-1 (Instructions to Offerors – Commercial Items) and 52.212-2 (Evaluation – Commercial Items). This matrix is a tool which helps ensure all the evaluation criteria and proposal submittal requirements identified in the solicitation have been responded to properly. The offeror shall fill out the cross reference matrix indicating where in their proposal the information can be found. Failure by the offeror to complete the matrix will result in the offeror being considered as failing to meet the RFP terms and conditions.

Start typing your response here and when done, remove all text that appears in gray - that is for your reference only

Evaluation Sub-Factors	Clause 52.212-1 – Para. #	IDIQ PWS Reference	TO 0001 PWS Reference	Clause 52.212-2 – Para. #	Proposal Volume, Section # and Page #
Technical					
Subfactor One: Cybersecurity Risk Management Framework Strategy					
Cybersecurity Risk Management Framework	5.2.1	2.1, 2.2, 2.3, 2.4, 2.7, 2.8, 2.10, 2.11, 6.5, 7.0, App B		3.1.1	
Security Coordination Center and Incident Response Center Service Provider	5.2.2	2.3, 2.6, 2.7, 7.0, App B		3.1.2	
Information Systems Security Training & ICD 502 and ICD 503	5.2.3	2.8, 7.0, App B		3.1.3	
Air Force Software certification	5.2.4	2.3, 2.5, 7.0, App B		3.1.4	
Systems Engineering	5.2.5	2.1, 2.3, App B		3.1.5	
Subfactor Two: Staffing Strategy					
Staffing Plan & Team Matrix	5.3.1	1.3, 6.5, App C		3.2.1	
DoD 8570.01M	5.3.2	2.0-2.11 App B		3.2.1	
Customer Service	5.3.3	2.6, 2.7		3.2.3	
Security Clearance Management	5.3.4	6.2		3.2.4	

Subfactor Three: Management Approach					
Personnel Retention Methods & IDIQ personnel management	5.4.1	2.0-2.11		3.3.1	
Personnel Management Plan	5.4.2	2.3, 2.6, 2.7		3.3.2	
Intellectual Property Management	5.4.3	2.1, 2.3		3.3.3	
Subfactor Four: Technical Overall Approach to the ACC/A2S-OL and 25 AF ISR RMF Support Task Order 0001					
Proposal Strategy to include Labor Mix	5.5.1	Attach 1 17 Sep 2015 TO 0001 (PWS)	Task Order PWS App C		
Technical Approach (PWS – TASK ORDER 0001)	5.5.2	Attach 1 17 Sep 2015 TO 0001 (PWS)	Task Order PWS 2.0 – 2.11		