USAC Security Controls Assessment

SOLICITATION INFORMATION:

Method of Solicitation:	Request for Proposal (RFP)
Award Effective Date:	TBD
Contract Period of Performance:	One (1) year with four (4) one-year renewable options
Solicitation Number:	IT-19-041
Solicitation Issue Date:	April 23, 2019
Offer Due Date:	May 6, 2019

CONTRACT TO BE ISSUED BY:

Universal Service Administrative Co.
700 12th Street, NW, Suite 900
Washington, DC 20005

CONTACT INFORMATION

USAC CONTACT INFORMATION	OFFEROR CONTACT INFORMATION
Ecatarina Grant Procurement Specialist III P: 202-772-4529 E: ecatarina.grant@usac.org	(complete) Name: _____ POC: _____ POC Title: _____ POC Phone: _____ POC Email: _____ Address: _____

OFFEROR SIGNATURE

_____ _____

Name and Title Date

SECTION A:
About Us and the Work

I. Overview of the Project

USAC is seeking a responsible Contractor to conduct a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls.

The USAC organization characteristics with respect to Information Security, include five (5) customer-facing business units that interact via web-based applications and application programing interfaces (APIs) with USF beneficiaries (schools, libraries, rural healthcare providers, low-income Lifeline subscribers), telecommunications service providers, and USF stakeholders. Each of these business units has no more than five (5) key systems. The majority of these systems are custom-built and on-premise. More recent systems are managed in third party vendors' cloud environments.

The Business Support Units (Human Resources, Audit, General Counsel, and Information Technology) rely mostly on Commercial Off the Shelf (COTS) based support systems that are configured to meet business unit requirements.

The selected Contractor will support these business units. In calendar year 2019, USAC expects the selected Contractor to perform a Security Controls Assessment (SCA) work for up to four (4) systems undergoing authorization efforts for the first time, as well as the assessment of 1/3 controls as part of continuous monitoring (CM) for six (6) systems. In calendar year 2020, USAC expects the selected Contractor to perform a Security Controls Assessment (SCA) work for up to four (4) systems undergoing authorization efforts for the first time, as well as the assessment of 1/3 controls as part of CM for six (6) systems. In calendar year 2021, USAC expects the selected Contractor to perform a Security Controls Assessment (SCA) work for up to four (4) systems undergoing authorization efforts for the first time, as well as the assessment of 1/3 controls as part of CM for six (6) systems. In all subsequent years, USAC expects the selected Contractor to perform assessment of 1/3 controls as part of CM for six (6) systems. These assessments will be in line with the USAC CM plan with the annual 1/3 controls and key controls

II. Background

Through its administration of the Universal Service Fund ("USF") programs on behalf of the Federal Communication Commission ("FCC"), USAC works to promote the availability of quality services at just, reasonable, and affordable rates, and to increase access to advanced telecommunications services throughout the nation. Specifically, the USF programs provide

funding for the expansion of telecommunications and broadband access to rural communities and health care facilities, schools and libraries across the country, and low income households. Through program administration, auditing, and outreach, USAC works with contributors, service providers, and program beneficiaries to achieve the program goals articulated by the FCC for each of these programs.

The FCC has reformed the USF to support further investment in and access to evolving broadband infrastructure, making the programs a primary vehicle to support this critical national priority. USAC, as the administrator of the USF, plays a critical role in supporting the ambitious vision to ensure that all citizens in the United States have access to high-speed broadband. The organization has approximately 500 employees. USAC works in close partnership with the FCC and other federal and state partners to support the achievement of the USF program goals.

USAC also administers the USF programs—High Cost, Lifeline, Rural Health Care, and Schools and Libraries. USAC strives to provide efficient, responsible stewardship of the programs, a key national asset in making important telecommunications and Internet services available to consumers, health care providers, schools, and libraries throughout the United States. The program divisions are supported by additional USAC personnel in Finance, General Counsel, Information Systems, Internal Audit, the Enterprise Program Management Office and Human Resources.

Consistent with FCC rules, USAC does not make policy for or interpret unclear provisions of statutes or the FCC's rules. Universal service is paid for by contributions from telecommunications carriers, including wireline and wireless companies, and interconnected Voice over Internet Protocol providers, including cable companies that provide voice service, based on an assessment of their interstate and international end- user revenues. These contributions are most typically passed through to consumers through a universal service fee line item on their telephone bills.

High Cost Program

The High Cost Program is dedicated to preserving and advancing voice and broadband service, both fixed and mobile, in rural areas of the United States. The High Cost Program ensures that rates for broadband and voice services are reasonably comparable in every region of the U.S. Like all USF programs, the administration of the High Cost Program has undergone significant modernization in the last several years to increase innovation and ensure beneficiaries have access to updated technology. USAC is leveraging the new High Cost Universal Broadband Portal ("HUBB"), which allows Carriers participating in modernized Connect America programs to file deployment data showing where they are building out mass-market, high- speed internet service by precise location. This information includes latitude and longitude coordinates for every location where service is available, and USAC will eventually display this information on a public-facing map to show the impact of Connect America funding on broadband expansion throughout rural America.

Low-Income (Lifeline) Program

The Lifeline Program provides a monthly discount on landline or wireless phone service to eligible low- income households. USAC works to ensure program integrity by making measurable and vital progress towards reducing program inefficiencies and waste while supporting the needs of Lifeline Program stakeholders through a detailed understanding of their challenges. To combat fraud, waste, and abuse, USAC reviews processes regularly to increase compliance, identify avenues for operational improvements, and refine program controls, such as audit processes. USAC has focused on data analytics to improve customer service and outreach approaches and increase the reach and effectiveness of the program to better serve service providers and subscribers. USAC is in the process of building the National Verifier, which will include the national Lifeline Eligibility Database to determine subscriber eligibility. USAC also operates the National Lifeline Accountability Database ("NLAD") which prevents duplicate scribers from receiving support in the Lifeline program.

Schools and Libraries (E-rate) Program

The Schools and Libraries program helps schools and libraries obtain high-speed Internet access and telecommunications at affordable rates. Recent E-rate Modernization Reform efforts focused on broadband to and within schools and libraries to support a modern and dynamic learning environment for all students. In support of improved program outcomes, USAC is completing the E-rate Productivity Center ("EPC") which enables electronic participation in the reformed Schools and Libraries Program. E-rate program funding helps ensure connectivity for schools and libraries across the country. USAC is investing in new tools and data analytics capabilities to support the success of the program in alignment with the FCC's goals.

Rural Health Care (RHC) Program

The Rural Health Care Program supports health care facilities in bringing medical care to rural areas through increased connectivity. The Rural Health Care Program provides reduced rates for broadband and telecommunications services via the Healthcare Connect Fund Program and Telecommunications Program. These telecommunications and broadband services are necessary to support telemedicine and allow cutting edge solutions and treatments to be accessible to Americans residing in rural areas.

Additional information on USAC programs can be found at:
http://www.usac.org/about/about/who-we- are/default.aspx

III. Goals

USAC is seeking a third party independent assessor for Assessment &Authorization services for compliance with FISMA/NIST Risk Management Framework (RMF) in order to obtain and maintain Authorization to Operate (ATO) for USAC systems.

SECTION B:
Requirements and Scope of Work

I. OVERVIEW OF THE USAC SECURITY CONTROLS ASSESSMENT EFFORT

As a part of USAC's ongoing efforts to improve IT security, USAC is seeking a responsible, independent Security Controls Assessor (SCA) Contractor for its ongoing Information Security Continuous Monitoring (ISCM) program. The Contractor will be responsible for ensuring that current USAC ATO for all accredited systems are maintained in accordance with the NIST Risk Management Framework (RMF) 800-37 rev 1.

The Contractor is also responsible for performing independent security control assessments in accordance with the NIST RMF 800-37 for any system(s) that currently do not have an ATO and for all future USAC system(s) as needed.

These activities include but are not limited to the following RMF Process:

A. Step 4 – Assess Security Controls: Determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements

   - Step 4-1: Develop, review, and approve a plan to assess the security controls.
   - Step 4-2: Assess the security controls in accordance with NIST, FISMA and USAC the assessment policies and procedures defined in the security assessment plan.
   - Step 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.
   - Conduct independent vulnerability scan using Nessus standalone.

B. Step 6-2: Assess a selected subset of the technical, management, and operational security controls in compliance with USAC Continuous Monitoring policy employed within and inherited by the information system in accordance with the USAC-defined continuous monitoring strategy.

II. TYPE OF CONTRACT

This is a single award, firm fixed price contract (Contract). USAC intends to award the Contract to one (1) contractor under this procurement. The firm fixed price is to include all direct and indirect costs set forth in this Section B, including equipment, product support, supplies, general and administrative expenses, overhead, materials, travel, labor, taxes

(including use and sales taxes), shipping, and profit. USAC will not reimburse Contractor for any travel-related expenses.

III. CONTRACT TERM

The term of this Contract shall be for one (1) year with four (4) one-year renewable options (Contract Term). The terms of the Contract shall commence on the Effective Date on which the Contract is signed.

USAC may require continued performance of any services required under the Contract (Services) beyond the expiration of the Contract Term, or any period included in the Contract Term, within the limits and at the rates specified in the Contract. USAC may extend the Services more than once, but the total extension of performance under the Contract shall not exceed six (6) months.

IV. PLACE OF PERFORMANCE

A. All required Contract services must be performed within the United States at the Contractor site, or USAC Corporate Headquarters at 700 12th Street NW, Suite 900, Washington, DC 20005 (USAC Headquarters), as needed.

B. A Contract kick-off meeting will be held at USAC Headquarters. Status and other meetings may be held telephonically or in person, at USAC's discretion. USAC will NOT reimburse Contractor for any travel related expenses for kick-off, status, and other meetings.

C. Services requiring work at USAC Headquarters, will include appropriate work space and appropriate access to USAC's computer network. No hardware will be provided. **NOTE**: **Contractor personnel requiring access to USAC IT Systems will be required to sign USAC's IT Security Rules of Behavior Form and complete mandatory IT Security and Privacy Awareness Online Training. Contractor may be required to complete Role-Based Privacy Act Training if accessing USAC information systems designated as Federal systems of record.**

D. Status update meetings and other meetings may be held onsite or virtually, except to the extent that USAC or the Contractor requires in-person presence. While attending USAC Headquarters for meetings, Contractor staff will be considered as visitors. All visitors are required to complete USAC's Visitor Form, USAC Visitor Form, and wear a badge while on premises. The Contract kick-off meeting and all in-person meetings will be held at USAC Headquarters or other reasonable locations designated by USAC.

V. PERFORMANCE REQUIREMENTS

The Contractor shall submit a project plan in MS Project within five (5) business day following the project kickoff meeting to USAC IT Security Director for approval. Contractor shall begin performance of Security Controls Assessment tasks no later than ten (10) business days following the project kick-off meeting (see section B.VII.A.1 below).

Contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success. Contractor service requirements, performance metrics, and remediation plans are provided in Table 2.

Table 1, USAC Performance Requirements

Performance Objective	Performance Threshold	Method of Surveillance
Contractor shall provide complete and on time Deliverables as described in the Contract.	The minimum acceptable Level shall be 100% of Deliverables on or before the due date.	100% Inspection: Based on direct observation by the USAC project manager (PM), Information System Security Officer (ISSO), etc. and input/discussion with customers and stakeholders
Contractor shall provide Deliverables, written and or presented, in a clear, concise, and technically accurate manner.	Work Products shall be clearly written, in a visually appealing style, information shall be organized in a logical manner, content shall be relevant, and the work product shall advance the goals of the program.	100% Inspection: Based on direct observation by the USAC PM, ISSO, etc. and input/discussion with customers and stakeholders
Contractor shall provide acceptable customer service including responsiveness to the contract needs and problem resolution.	Initial inquiry by phone, email, text or face-to-face contact: 1. Inquiry shall be acknowledged within 1 hour during the hours of 9:00 AM – 6:00 PM EST. 2. Contractor shall provide expected resolution time within eight (8) business hours. 3. Inquiry shall be resolved within resolution time provided by the Contractor. 4. Inquiry shall be adequately resolved to the customer's satisfaction	100% Inspection: Based on direct observation by the USAC PM, ISSO, etc. and input/discussion with customers and stakeholders
Contractor shall attend all required meetings as described in the Contract.	The minimum acceptable Level shall be 100% attendance at all required meetings.	100% Inspection: Based on direct observation by the USAC PM, ISSO, etc. and input/discussion with customers and stakeholders.

A. Steps in the Surveillance Process:

The surveillance process is driven by the USAC escalation process, which includes built-in quality assurance (QA). The QA process is designed to create automatic QA spot checks and provide an automatic escalation process.

1. Discrepancies are immediately elevated to USAC Procurement Department;
2. If the Deliverables match the Contract requirements and are executed according to both the format and level of detail required, the Deliverable is accepted;
3. Should Contractor's work be adjudicated as inadequate, normal payment of the invoice will be delayed until the Deliverables are compliant with the USAC requirements.

All Deliverables its elements and appendices, are considered Confidential Information (see Section C.XXVI) and are the sole property of USAC. USAC may use and disclose the Deliverables in its sole discretion. Each document Deliverable shall be submitted in an acceptable electronic unprotected format, using Microsoft® Excel, Microsoft® Word, Microsoft® Project Professional, PDF, or any other format that is mutually agreed upon by USAC and Contractor.

VI. SCOPE OF SERVICES AND DELIVERABLES

Contractor shall provide the following Services and Deliverables in accordance with terms set forth below and in Section C of this RFP:

A. *Deliverables Overview and Submission Requirements:* The Contractor is responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within USAC. The Contractor shall also provide an assessment of the severity of weaknesses or deficiencies discovered and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, SCAs prepare the final security assessment report (SAR) containing the results and findings from the assessment.

i. **Step 4 (TASK 1) –** Assess Security Controls: Determine the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements:
    a. Step 4-1 (TASK 1.1): Develop, review, and approve a plan to assess the security controls.
    b. Step 4-2 (TASK 1.2): Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.
    c. Step 4-3 (TASK 1.3): Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

ii. **Step 6-2 (TASK 2):** Assess a selected subset of the technical, management, and operational security controls in compliance with USAC Continuous Monitoring policy employed within and inherited by the information system in accordance with the USAC-defined continuous monitoring strategy.

B. Contractor shall provide the following Services detailed here:

1. RMF Step 4.1 (TASK 1.1) – Security Control Assessment Preparation:

a. Contractor shall collaborate with the System Owner (SO), Technical Lead (TL), and supporting staff to develop a System Rules of Engagement (ROE) Agreement. The ROE must correctly identify the following:
    1) Scope of testing;
    2) Network ranges being assessed;
    3) System components being assessed;
    4) Locations being assessed (primary on-site location, secondary on-site location(s) (if applicable) and remote assessment(s) (if applicable);
    5) SCA and all members conducting assessments including systems being used;
    6) Tools used for the assessment;
    7) Policy and processes regarding assessment interruptions due to unforeseen network, system component and mission impacts.

b. Contractor shall develop and submit a Security Control Assessment Work Plan (SCAWP) which shall:
    1) Identify and document the appropriate security assessment level of effort and project management information to include tasks, reviews (including compliance reviews), resources, and milestones for the system being tested;
    2) List key resources necessary to complete the security control assessment, including tools and Contract support for the required activities
    3) List key roles and personnel participating in security assessment activities
    4) Include an overall assessment process flow or swim-lane diagram which documents the steps required to conduct assessment activities and interact with all necessary parties (including but not limited to: Chief Information Officer (CIO), Director of Information Security (DIS), Information Technology Security Officer (ITSO), Authorization Officer (AO), Security Officer (SO), Information Systems Security Officer (ISSO), Project Manager (PM), Security Controls Accessor (SCA)).

c. Contractor shall develop and document an RMF Security Assessment Plan (SAP) and perform the SCA according to the SAP. The SAP shall include a complete and comprehensive description of all processes and procedures Contractor will perform. Developed and documented processes and procedures to be performed by Contractor shall:

    1) Include a sequential, step-by-step description of all actions required to perform each assessment;

2) Provide a sufficient level of detail to ensure any knowledgeable and experienced security professional could perform the same procedure and obtain the same results;
3) Allow for updates to the process and procedures to correct misinterpretation of security controls assessment procedures;
4) Address federal legislation (e.g. FISMA), OMB, NIST Special Publications (SP), Federal Information Processing Standards (FIPS) and USAC policies, standards, guidance, and required templates. USAC will provide the IT Policy and Guidance Timeline Requirements to address when new policies, directives, and guidance are to be used;
5) Comply with NIST Special Publications 800-37, Rev. 1 or Rev.2 RMF, SCA activities as defined in the latest version of NIST Special Publications;
6) Leverage and utilize a working knowledge of existing, new, and revised "final" publications (Appendix A) and best practices when developing security control assessment procedures. Working knowledge would be obtained by reviewing all of the NIST Publications and Standards and then applying this knowledge when developing the assessment procedures. For example, if assessing AT-2 Security Awareness and AT-3 Security Training (Awareness and Training Family) security controls, the assessment process and procedures must incorporate the NIST SP 800-16 & 800-50 definitions for security awareness and security training;
7) Allow for changes to address updates and revisions from federal legislation, OMB, NIST, and USAC policies, guidance, and required templates;
8) Address all system components identified within the system boundary;
9) Identify what commands (applications/tools) are executed on each unique system component an include an explanation/ description of how the SCA utilized the information generated by commands;
10) Account for appropriate assessment procedures to address the rigor, intensity, and scope of the assessment based on the following three (3) factors:
11) System Security Categorization (RMF Task 1);
12) Assurance requirements that the organization intends to meet in determining the overall effectiveness of the security controls (RMF Task 3);
13) Selection of security controls from Special Publication 800-53 as identified in the approved security plan (RMF Task 2).
14) Address the collection and/or generation of security controls assessment artifacts, including a description of:

a. When the Security Controls Assessor (SCA) will witness Artifact collection;
b. When and under condition Artifacts collected is accepted when not witnessed by SCA;
c. How artifacts are delivered (i.e. transfer method for electronic/digital) to the SCA from the SO team.

15) Ensure system component/device identification is tracked across all artifacts and assessment evidence in order to support assessment and findings activities (e.g., IP address, hostname, etc.);
16) Ensure a review checklist process to identify documents submitted in the SO's System Security Package which do not comply with the latest USAC required templates;
17) Account for all locations and system components identified in the system boundary and system inventory; and
18) Incorporate the development and approval for the ROE Agreement.

d. Contractor shall have USAC review and approve all processes and procedures, including modifications to existing processes and procedures incorporated from lessons learned, to streamline and improve RMF activities.

e. Contractor shall complete the following communication and reporting activities:

1) Assessment and Deliverables Schedule: Provides a detailed description of all assessment and Deliverable milestones;
2) SO Memorandum: Requests security controls assessment and System Security Package (SSP) contents and describes the purpose of the SSP assessment and SSP contents submitted for assessment;
3) SCA Memorandum: Acknowledges and identifies any discrepancies related to the SO SSP, including the purpose of the SSP assessment, lists the files submitted for assessment, and documents any discrepancies identified by the SCA in the documentation provided; and
4) System Component Assessment Schedule: Includes primary on-site location, secondary on-site location(s) (if applicable), remote assessments (if applicable), date, time, participating staff, and component scheduled for assessment (e.g., servers, workstations, network equipment).

2. RMF Step 4.2 (TASK 1.2) – Security Control Assessment:

Contractor shall complete the following communication and reporting activities:

a. *System Component Assessment Kickoff Meeting:* Addresses all components being assessed, primary on-site location, secondary on-site location (if applicable), Disaster Recovery Site (if applicable), and remote assessments (if applicable)

b. *System Component Assessment Weekly Status:* Conducts a verbal discussion/meeting to address progress for currently completed and/or pending system component assessments (scanning and hands-on), including:

1) Number of, role, and names of necessary USAC personnel to be interviewed for control assessment(s);
2) Vulnerability scanning;
3) Penetration testing (if applicable);
4) Hands-on assessment;
5) Any other system component assessment (if applicable);
6) All system components being assessed;
7) Primary on-site location;
8) Secondary on-site location(s) (if applicable);
9) Remote assessments (if applicable);
10) Total number of system components being assessed broken into each unique system component type (e.g., 10 Servers, 25 Workstation/Laptops, 3 Routers, etc.);
11) Total number of system components completed per unique system component type;
12) Total number of system components remaining/pending per unique system component type to meet the required assessment;
13) Percentage of completion per unique system component type; and
14) System Component Out-Brief Meeting: Held at primary on-site location to summarize preliminary findings (i.e., raw findings without analysis) and address:
    a. All interviews with required USAC personnel
    b. All system components assessed;
    c. Primary on-site location;
    d. Secondary on-site location(s) (if applicable);
    e. Remote assessments (if applicable);
    f. Vulnerability scanning;
    g. Penetration testing (if applicable);
    h. Hands-on assessment; and

i. Any other system component assessment (if applicable).

3. **RMF Task 4.3 (TASK 1.3) – Security Assessment Report:** The Contractor shall develop the SAR to include the following:
    a. Documentation of each security control assessment;
    b. Assessment test objectives as identified in NIST SP 800-53A;
    c. Assessment test types (e.g., interview, examine, test) as identified in NIST SP 800-53A;
    d. All software and hardware components assessed;
    e. Sequential, step-by-step assessment procedures for testing each test objective (i.e., procedures Contractor will follow when assessing each test objective of each security control for consistency and repeatability);
    f. Results of control assessment, evaluation, and analysis of the system within the defined system boundary, supporting infrastructure, and operating environment;
    g. Evidence that all components in the System Inventory were tested or covered by a test performed on a representative sample of identically configured devices;
    h. Rationale for any system or device in the inventory not directly tested (e.g., if the system is in maintenance, deployed, or being disposed of, the risk of not testing this system must be addressed in the SAR);
    i. Results that ensure configuration settings for all major IT products in the system were assessed, identifying each system component, secure benchmark assessed, location of scan results, confirmation the assessed component implements approved organizational, defined, secure benchmark;
    j. Determination that the security control is "Satisfied" or "Other Than Satisfied" with each sequential step of the assessment process providing a "Satisfied" or "Other Than Satisfied" determination (e.g., if the Contractor is assessing a control that has four assessment steps, each step must assign "Satisfied" or "Other Than Satisfied" findings to assist the SO in developing the appropriate mitigation of the finding);
    k. A finding of "Satisfied" indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., collected evidence) indicates the assessment objective for the control has been met, producing a fully acceptable result;
    l. A finding of "Other Than Satisfied" indicates that for the portion of the security control addressed by the determination statement, the assessment information obtained indicates potential anomalies in the operation or implementation of the security control;

m. Actual, unbiased, and factual results and analysis used to make final determinations that the security control is "Satisfied" or "Other Than Satisfied" with actual results for each system component type. If "Other Than Satisfied" is determined for a security control, then further details shall be provided indicating if the control is not implemented, partially implemented, inherited, or otherwise how the determination of "Other Than Satisfied" was reached; and

n. Identification and explanation for all artifacts used in the assessment, as generated or provided by the SO, with the following information:

   a. File name, including security control (e.g., AC-1), FISMA system, and context (e.g., screen shot);
   b. Location of the artifact(s);
   c. Security control the artifact(s) supports; and
   d. Clear description within artifacts in order to support "Satisfied" or "Other Than Satisfied" findings; for "Other Than Satisfied" findings, the Contractor shall also describe how the control differs from the planned or expected state.

4. **Reports:** Contractor shall provide all documentation developed to support assessment, artifact collection, findings, analysis, conclusions, management recommendations, and reports:

   a. SCA electronic, digital, audio, video, and/or hand-written information used in collecting, tracking, and/or analyzing assessment activities;
   b. All observations with a clear description of how, who, what, when, and where as well as how the observation "Satisfies" or "Other Than Satisfies" the requirement of the assessment objectives in the SAR;
   c. Tracking spreadsheet to track system components being assessed;
   d. Output (raw or native tool) generated from assessment tools to allow import by the SO team into the same tool for mitigation (e.g., Nessus formatted file);
   e. Vulnerability Assessment Report (VAR) to document the scan-to-inventory analysis, determination regarding use of authentication in scanning, and analysis of scan results;
   f. Penetration Testing Report (if applicable) to document the results of penetration;
   g. Summary of findings of these detailed reports to develop a SAR; and
   h. Updates and/or additions generated from Lessons Learned activities.
   i. Contractor shall complete the following communication and reporting activities:

2) **Technical Briefing:** Present SCA findings, vulnerabilities, and penetration results with analysis, conclusions, and recommendations to SO, SO staff, DIS, ISSO, ITSO, IT Staff, and others as needed.

3) **Management Briefing:** Present findings, vulnerabilities, and penetration results, focusing on the risk and residual risk issues. Provide analysis, conclusions, and recommendations for system operations (ATO or Denial of Authorization to Operate) to SO, SO staff, DIS, ISSO, ITSO, IT Staff, and others as needed. Briefing slides should summarize:

   i. Key information about the system (e.g., system mission/purpose, security categorization, information types that are drivers for the high water-mark categorization, facility locations, and number of components in the official inventory);
   ii. Purpose of the SSP assessment and list of files submitted for assessment;
   iii. Scope and methodology from the SAP as well as scope limitations/restrictions encountered during the assessment as described in the SAR;
   iv. Assessment results as detailed in the SAR, Security Controls Assessment (Test) Procedures and Results, and the Continuous Monitoring Annual Security Controls Assessment;
   v. Discussion of risk and residual risk of operating the system in its current environment, and discuss the recommendation for acceptance of risk;
   vi. Contractor shall work with the ITSO and ISSO to prepare a list of possible AO questions related to POA&Ms and assessment findings to fully understand weaknesses;
   vii. Contractor shall work with the ITSO and ISSO prior to the AO briefing to ensure a consistent understanding of findings and to develop draft determination of risk;
   viii. Contractor shall verbally respond to AO questions, along with the ITSO and ISSO, to assist with the determining of risk to organizational operations (mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation; and
   ix. The AO will assess the information and in collaboration with the ITSO, ISSO, and Contractor, document the AO risk approach.

4) **Lessons Learned:** Contractor shall develop and update Lessons Learned from A&A activities and incorporate these into processes and procedures as applicable. Feedback on Lessons Learned should be collected from, but not limited to, the following individuals prior to incorporating into existing processes and procedures:
    i. Authorizing Official (AO);
    ii. System Owner (SO);
    iii. Director of Information Security (DIS);
    iv. Director of Privacy (DoP);
    v. Information System Security Officer (ISSO);
    vi. IT System Owner (ITSO);
    vii. Security Controls Assessor (SCA);
    viii. Program Manager (PM); and
    ix. Contracting Officer (CO).

5. RMF Task 6.2 (TASK 2) – Ongoing Security Control Assessments:

Contractor shall

a. Contractor shall develop a Continuous Monitoring Security Controls Assessment Plan and Schedule. This plan should include required activities and outputs required by RMF Tasks 4.1, 4.2, and 4.3.
b. Contractor shall perform Continuous Monitoring Annual Security Controls Assessments according the Continuous Monitoring Security Controls Assessment Plan and Schedule.
c. Contractor shall perform all required communications and reporting activities as required by RMF Tasks 4.1, 4.2, and 4.3.

C. Deliverables*:*

Contractor shall provide the following Deliverables and supporting documentation. Contractor shall respond to any inquiries regarding Deliverables required in responding to potential system audits (e.g., USAC Internal Audit, FCC Officer of the Inspector General) within one (1) year of Deliverable completion and approval. All Contract Deliverables are described in Table 1 below.

Table 2, USAC SCA Deliverables

RMF	Deliverable	Frequency	Medium/Format	Deliver To
4-1 & 6.2	System Rules of Engagement (ROE) Agreement	TBD	MS Word	PM, SO, ISSO, COR
4-1 & 6.2	Security Control Assessment Work Plan (SAWP)	TBD	MS Word	PM, SO, ISSO, COR
4-1 & 6.2	Security Assessment Plan (SAP)	TBD	MS Word	PM, SO, ISSO, COR
4-1 & 6.2	Assessment/Deliverables Schedule	TBD	MS Project	PM, SO, ISSO, COR
4-1 & 6.2	SO Memorandum	TBD	MS Word	PM, SO, ISSO
4-1 & 6.2	SCA Memorandum	TBD	MS Word	PM, SO, ISSO
4-1 & 6.2	System Component Assessment Schedule	TBD	MS Project	PM, SO, ISSO, COR
4-2 & 6.2	System Component Assessment Kickoff Meeting	TBD	In-Person	PM, SO, ISSO, COR
4-2 & 6.2	System Component Assessment Daily Status	TBD	Verbal	PM, ISSO
4-2 & 6.2	Weekly Report	TBD	MS Word	PM, SO, ISSO, COR
4-2 & 6.2	System Component Out-Brief Meeting	TBD	In-Person	PM, SO, ISSO, COR

RMF	Deliverable	Frequency	Medium/Format	Deliver To
4-3 & 6.2	Security Assessment Report (SAR)	TBD	MS Word (with corresponding tables in Excel, if applicable)	PM, SO, ISSO, DIS
4-3 & 6.2	Assessment Documentation	TBD	MS Word (with corresponding tables in Excel, if applicable)	PM, SO, ISSO, DIS
4-3 & 6.2	Technical Briefing	TBD	In-Person/Verbal	PM, SO, ISSO, DIS
4-3 & 6.2	Management Briefing	TBD	In-Person/Verbal	PM, SO, ISSO, DIS
4-3 & 6.2	Lessons Learned	TBD	MS Word	PM, SO, ISSO, COR
6-2	Continuous Monitoring Security Controls Assessment Schedule	TBD	MS Project	PM, SO, ISSO, DIS
N/A	USAC Kick Off Meeting	TBD	In-Person	PM, SO, ISSO, COR
N/A	Weekly Meeting	TBD	In-Person/Verbal	PM, SO, ISSO

Table 3, USAC SCA Milestone Timetable

No. of Systems	Task Activity	Due Date
2019 Milestones		
3	ISCM	June 30, 2019
1	ISCM	July 31, 2019
2	ISCM	October 15, 2019
2	ATO	September 30, 2019
2020 Milestones		
3	ISCM	June 30, 2020
2	ISCM	September 30, 2020

2	ISCM	October 15, 2020
1	ATO	March 30, 2020
2	ATO	December 31, 2020
2021 Milestones		
3	ISCM	June 30, 2021
2	ISCM	September 30, 2021
2	ISCM	October 15, 2021
1	ISCM	March 30, 2021
2	ISCM	December 31, 2021
2022 Milestones		
3	ISCM	June 30, 2022
2	ISCM	September 30, 2022
2	ISCM	October 15, 2022
1	ISCM	March 30, 2022
2	ISCM	December 31, 2022
2023 Milestones		
3	ISCM	June 30, 2023
2	ISCM	September 30, 2023
2	ISCM	October 15, 2023
1	ISCM	March 30, 2023
2	ISCM	December 31, 2023

All Deliverables, including weekly reports, are considered Confidential Information (see Section C. XIV) and are the sole property of USAC. USAC may use and disclose the Deliverables at its sole discretion.

All Deliverables shall be placed in the USAC Information Security SharePoint site repository in a designated location. This process will continue until the end of the engagement.

D. Quality Assurance:

Contractor shall ensure quality assurance in accordance with the Contract. Contractor shall develop and implement procedures specific to the requirement to identify, prevent, and ensure non-recurrence of defective Services. Contractor's quality assurance program is the means by which the SCA contractor ensures the work complies with the requirements as requested. At a minimum, Contractor shall develop quality assurance procedures that address the areas identified in the Section B.V – Performance Requirements section above.

The USAC Contract Specialist shall pursue remedies for Contractor's failure to perform satisfactory Services or failure to correct non-conforming Services in accordance with the terms and conditions of the Contract.

The USAC Contract Specialist, in conjunction with USAC information security team, will ensure Contractor adheres to standard A&A methodologies, provided to ensure adequate performance and quality across A&A activities and Deliverables, and provide visibility across USAC enterprise risks.

USAC will:

- Coordinate A&A Services in conjunction with the DIS and USAC program teams to support ATO determinations;
- Provide liaison Services between the USAC system teams and Contractor;

Ensure SO and/or SO staff do not interfere or attempt to influence SCA assessments or findings;

VII. MEETINGS/MANAGEMENT AND KEY PERSONNEL

A. **Meetings.**

1. *Project Kick-Off Meeting*.

i. Within five (5) business days of the Contract start date, Contractor shall initiate work on this Contract by meeting with key USAC representatives to ensure a common understanding of the requirements, expectations, and ultimate end products. Contractor shall discuss the overall understanding of the project and review the background information and materials provided by USAC.

ii. Discussions will also include the scope of work, Deliverables to be produced, how the efforts will be organized and how the project will be conducted.

2. *Accessibility*: Key Personnel must be available via telephone or email during standard business hours, Monday through Friday (8:00 AM – 6:00 PM EST).

B. Key Personnel. Contractor shall provide staffing for the sample labor categories below, or Contractor may propose other labor categories in its proposal submission. Any additional labor categories must include the associated labor hour bill rate for each additional category submitted as well as the experience and qualifications of the personnel to be assigned to that labor category. Contractor shall assign, as Key Personnel, at least one of each of the following:

1. ***Project Manager*** (PM) whose primary duties will be the implementation and oversight of the project. The Project Manager shall act as the primary point of

contact for Contract administration issues which include but are not limited to addressing billing and reporting issues and assisting the Contractor and USAC in the event of any planned or unplanned outages. The Project Manager shall participate in weekly, quarterly, and yearly teleconference status meetings with USAC to review verifications and discuss any new and/or outstanding issues. The Project Manager shall provide USAC with any other support necessary for performance of the Contract requirements.

2. A ***Lead Assessor*** whose primary duties will be to ensure that all requirements for assessment in compliance with NIST are being met for USAC systems. The Lead Assessor will play a key part in validating all work provided to USAC by the Contractor and ensuring that the quality assurance requirements have been met. In addition, the Lead Assessor will work with the assessment team (comprised of additional security controls assessors provided by Contractor) to ensure consistency in processes across all assessments performed at USAC. All security controls assessors must hold in good standings at least one of the following IT Professional Certifications (or equivalent):

    - GIAC Systems and Network Auditor (GSNA)
    - ISC2 Certified Authorization Professional (CAP)
    - ISC2 Certified Information System Security Professional (CISSP)
    - ISACA Certified Information System Auditor (CISA)

SECTION C:
USAC Terms and Conditions

I. DEFINITIONS

A. "Contractor" means the Offeror whose proposal was selected for award of the Contract.

B. "Data" means recorded information, regardless of form or the media on which it may be recorded, and includes, but is not limited to, technical data and Software.

C. "Deliverables" means the deliverables, goods, items, products, and material that are to be prepared by Contractor and delivered to USAC as described in Section B.

D. "Offeror" means an entity submitting a formal proposal in response to this Solicitation.

E. "Services" means the tasks, services, functions and responsibilities described in Section B and in the Contract issued hereunder.

F. "Software" means computer programs that allow or cause a computer to perform a specific operation or series of operations, together with all modifications to, or enhancements ("derivative works") thereof.

II. INSPECTION / ACCEPTANCE

Contractor shall only tender for acceptance Services and Deliverables that conform to the requirements of the Contract. USAC will, following Contractor's tender, inspect or test the Deliverables or Services and:

(a) Accept the Services and Deliverables; or

(b) Reject the Services and Deliverables and advise Contractor of the reasons for the rejection.

If rejected, Contractor must repair, correct or replace nonconforming Deliverables or re-perform nonconforming Services, at no increase in Contract price. If repair, correction, replacement or re-performance by Contractor will not cure the defects or is not possible, USAC may terminate for cause under Section C.XI, below, and, in addition to any other remedies, may reduce the Contract price to deduct amounts for the defective work.

Unless specified elsewhere in the Contract, title to items furnished under the Contract shall pass to USAC upon acceptance, regardless of when or where USAC takes possession.

III. ENTIRE CONTRACT / BINDING EFFECT

The Contract, including the following contract documents listed in descending order of precedence: (1) Sections A-E, including the attachments identified in Section D; and (2) any other attachments – constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. Section B and Section C have priority and shall take precedence over any other Contract document, including Contractor proposals that may be included as attachments to the Contract. Any waiver of any provision of the Contract will be effective only if in writing and signed by the party granting the waiver. The Contract shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and assignees.

IV. CHANGES

The terms of the Contract shall not be modified other than in writing signed by the parties. The parties may bilaterally modify the Contract as needed.

V. INVOICES

A. *Where to Submit Invoices.* Contractor shall submit invoices electronically to **Accounting@USAC.org**. Additionally, Contractor shall submit an electronic invoice to the address designated in the Contract to receive invoices.

B. *Invoice Content.* Invoices must include:
   1. Name and address of Contractor;
   2. Invoice date, number and period of performance;
   3. Contract number;
   4. Completed and signed copies of the Contractor Weekly Status Report and Time Sheet by each Contractor personnel performing services on the Contract for the time period covered by the invoice, if applicable;
   5. Name and address of official to whom payment is to be sent or to notify in event of invoice or payment issues; and
   6. Any other substantiating documentation or information as reasonably required by USAC.

C. *EFT Information*. Contractor shall provide Electronic Funds Transfer (EFT) banking information via secure method prior to issuance of first invoice. USAC shall not be liable for incomplete or erroneous transfers which occur as a result of Contractor providing incorrect or out of date EFT information.

D. *Invoice Submittal Date.* Contractor may submit invoices for payment upon completion and USAC's acceptance of all of the work associated with a Contract or, if the period of performance of a Contract exceeds sixty (60) days, once every thirty (30) days, with the submission of the first invoice no earlier than thirty (30) days after issuance of the Contract.

E. *Content of Periodic Invoices.* If periodic invoices are submitted for a Contract, each invoice shall include only services that have been completed and Deliverables that have been accepted as of the date of invoice submission and that have not been billed in a prior invoice.

F. *Contractor Statement to Accompany Invoices.* All invoices shall be accompanied by the following statement signed by Contractor: "I certify that the services and items submitted on this invoice have been performed and delivered in accordance with the Contract [insert contract number] and that all charges are true, correct and have not been previously billed."

VII. PAYMENT / RATES

Contractor shall be paid for services performed on a fixed-price, service category rate basis using the service categories and fixed rates set forth in **Attachment 1**. USAC will pay invoices submitted in accordance with Section C.V., above, within thirty (30) calendar days of receipt of invoice, provided the Services and/or Deliverables have been delivered and accepted by USAC. The labor rates are firm and shall remain firm unless agreed to in writing by the parties, or unless Contractor provides a rate reduction or discount thereto. All labor rates specified herein are fully loaded and include all direct and indirect costs and expenses, including applicable federal, state, or local sales, use, or excise taxes, and profit.

VIII. PATENT INDEMNITY

Contractor shall indemnify, hold harmless and defend USAC and its directors, officers, employees and agents against any and all claims and liability, including attorney's fees and other costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, or misappropriation of, any patent, trademark or copyright, arising out of or related to Contractor's performance of the Contract.

IX. ASSIGNMENT / SUBCONTRACTING

Contractor shall not assign or subcontract all or any portion of the Contract without obtaining USAC's prior written consent. Consent must be obtained at least thirty (30) days prior to the proposed assignment or subcontracting. USAC may require information and assurances that the proposed assignee or subcontractor has the skills, capacity, qualifications and financial strength to meet all of the obligations under the Contract. An assignment or subcontract shall not release the Contractor of the obligations under the Contract, and the assignee or subcontractor shall be jointly and severally liable with the Contractor. Contractor shall not enter into any subcontract with a company or entity that is debarred, suspended, or proposed for debarment or suspension by any federal executive agency unless there is a compelling reason to do so. Contractor shall review the System for Award Management ("SAM") for suspension or debarment status of proposed subcontractors. *See* https://www.sam.gov.

X. TERMINATION FOR CONVENIENCE

USAC may terminate the Contract for any reason or no reason upon one (1) day prior written notice to the Contractor. Subject to the terms of the Contract, Contractor shall be paid for all time actually spent performing the Services required by the Contract up to date of termination, plus reasonable charges Contractor can demonstrate to the satisfaction of USAC have resulted directly from the termination.

XI. TERMINATION FOR CAUSE

Upon the expiration of a ten (10) day cure period (during which the defaulting party did not provide a sufficient cure), the non-defaulting party may terminate the Contract issued hereunder, in whole or in part, *for cause* in the event of the defaulting party's failure to comply with any material term or condition of the Contract, as applicable, or if either party fails to provide the other party, upon request, with adequate assurances of future performance. In the event of termination for cause, the non-defaulting party shall be entitled to any and all rights and remedies provided by law or equity. If it is determined that USAC improperly terminated the Contract for cause, such termination shall be deemed a termination for convenience. In the event of partial termination, the defaulting party shall continue to perform the portion of the Services not terminated.

XII. STOP WORK ORDER

USAC may, in its sole discretion, issue a stop work order at any time during the Contract term. Upon receipt of a stop work notice, or upon receipt of a notice of termination (for cause or convenience), unless otherwise directed by USAC, Contractor shall, on the stop work date identified in the stop work or termination notice: (A) stop work, and cause its subcontractors, consultants or agents to stop work, to the extent specified in said notice; and (B) subject to the prior written approval of USAC, transfer title and/or applicable licenses to use, as appropriate, to USAC and deliver to USAC, or as directed by USAC, all materials, Data, work in process, completed work and other USAC Information or material produced in connection with, or acquired for, the work terminated. In the event of a stop work order, all deadlines in the Contract shall be extended on a day for day basis from such date, plus reasonable additional time, as agreed upon between the parties, acting in good faith, to allow Contractor to reconstitute its staff and resume the work.

XIII. LIMITATION OF DAMAGES

Except in cases of gross negligence or willful misconduct, in no event shall either party be liable for any consequential, special, incidental, indirect or punitive damages arising under or relating to the performance of the contract. USAC's entire cumulative liability from any causes whatsoever (including indemnification obligations, if any), and regardless of the form of action or actions, whether in contract, warranty, or tort (including negligence), arising under the contract shall in no event exceed the lesser of Contractor's actual, proven direct damages or the amounts paid to Contractor under the contract. The parties expressly acknowledge that the limitations and exclusions set forth in this provision have been the subject of active and complete negotiation between the parties and represent the parties' agreement based upon the level of risk to the parties associated with their respective obligations under the contract and the payments provided hereunder to Contractor for its performance of the Services and Deliverables. All exclusions or limitations of damages contained in the contract, including, without limitation, the provisions of this section, shall survive expiration or termination of the Contract.

XIV. CONFIDENTIAL INFORMATION

A. *Confidential Information*. Confidential Information includes, but is not limited to, information, Data, material, or communications in any form or format, whether tangible or intangible, spoken or written (collectively referred to hereafter as "Information"), that contains, reflects, or is derived from or based upon, or is related to:

1. Management, business, procurement or financial Information of either party, the FCC or a USF stakeholder, including proprietary or commercial Information and trade secrets that have not previously been publicly disclosed;

2. Information regarding USAC's processes and procedures (including, but not limited to, program operational Information, Information regarding USAC's administration of its programs, and Information regarding USAC's processing of applications for program support);

3. Information concerning USAC's relationships with other vendors or contractors, the FCC, USF Stakeholders and financial institutions;

4. Information marked to indicate disclosure limitations such as "Confidential Information," "proprietary," "privileged," "not for public disclosure," "work product," etc.;

5. Information compiled, prepared or developed by Contractor in the performance of the Contract; the foregoing shall not include Information that is already lawfully in the possession of the recipient party prior to the receipt of such Information;

6. Any Information identified as confidential by the disclosing party; and

7. Personally Identifiable Information (PII), any information about an individual that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII include name, address, telephone number, date and place of birth, mother's maiden name, biometric records, etc.

B. *Non-Disclosure/Use/Irreparable Harm*. It is anticipated that one of the parties (Disclosing Party) may disclose, or has disclosed, Confidential Information to the other party (Recipient). At all times during the term of the Contract and thereafter, the Recipient shall maintain the confidentiality of all Confidential Information and prevent its unauthorized disclosure, publication, dissemination, destruction, loss, or alteration. Recipient shall only use Confidential Information for a legitimate business purpose of USAC and in the performance of the Contract. Recipient acknowledges that the misappropriation, unauthorized use, or disclosure of Confidential Information would cause irreparable harm to the Disclosing Party and could cause irreparable harm to the integrity of the USF Programs.

C. *Employee Access to Confidential Information*. Recipient shall not disclose Confidential Information to partners, joint venturers, directors, employees, agents and subcontractors (sub-Recipient) unless absolutely necessary for a Recipient's or sub-Recipient's performance of the Contract, and if necessary, shall only disclose the Confidential Information necessary for sub-Recipient's performance of its duties. As a pre-condition to

access to Confidential Information, Recipient shall require sub-Recipients, including its employees and subcontractors, and the employees of any subcontractor, to sign a non-disclosure or confidentiality agreement containing terms no less restrictive than those set forth herein. The Disclosing Party may enforce such agreements, if necessary, as a third-party beneficiary.

D. *Contractor Enforcement of Confidentiality Agreement*. Contractor must report, and describe in detail, any breach or suspected breach of the non-disclosure requirements set forth above to the USAC General Counsel immediately (i.e., within one (1) hour) upon becoming aware of the breach. Contractor will follow-up with the USAC General Counsel and provide information on when and how the breach occurred, who was involved, and what has been done to recover the Information.

E. *Exclusions*. If requested to disclose Confidential Information by an authorized governmental or judicial body, Recipient must promptly notify the Disclosing Party of the request and to the extent that it may legally do so, Recipient must refrain from disclosure of the Confidential Information until the Disclosing Party has had sufficient time to take any action as it deems appropriate to protect the Confidential Information. In the event Confidential Information of USAC is requested, Recipient must notify USAC, with a copy to USAC's General Counsel, of the request. Neither Contractor nor its subcontractors shall issue any public statement relating to or in any way disclosing any aspect of the Contract without the prior written consent of USAC. Notwithstanding anything herein to the contrary, USAC may, without notice to Contractor, provide the Contract, including Contractor's proposal information, and any information or Data delivered, prepared or developed by Contractor in the performance of the Contract to the FCC or other governmental or judicial body, and may publicly disclose basic information regarding the Contract, e.g., name of Contractor, price, basis for selection, description of Services/Deliverables and any provisions necessary for USAC to justify actions taken with respect to the Contract.

XV. RETURN OF USAC INFORMATION

A. "USAC Information" includes Information and Data provided by USAC to Contractor for use in the performance of the Contract, Data that is collected, developed or recorded by Contractor in the performance of the Contract, including without limitation, business and company personnel information, program procedures and program specific information, and Data that is created or derived from such Data. USAC Information is Confidential Information and subject to all requirements in Section C.XIV.

B. Promptly upon the expiration or termination of the Contract, or such earlier time as USAC may direct, Contractor shall, at the direction of USAC, and at no additional cost to USAC,

return or destroy all USAC Information, including all copies thereof, in the possession or under the control of Contractor. Contractor shall not withhold any USAC Information as a means of resolving any dispute. To the extent that there is a dispute between Contractor and USAC, Contractor may make a copy of such USAC Information as is necessary and relevant to resolution of the dispute. Any such copies shall promptly be destroyed upon resolution of the dispute.

C. USAC Information is provided to Contractor solely for the purpose of rendering the Services, and USAC Information or any part thereof shall not be sold, assigned, leased, or otherwise transferred to any third party by Contractor (except as required to perform the Services or as otherwise authorized in the Contract), commingled with non-USAC Information, or commercially exploited by or on behalf of Contractor, or its employees or agents. Promptly upon the expiration of the Contract term, or such earlier time as USAC may direct, Contractor shall, at the direction of USAC, and at no additional cost to USAC, return or destroy all copies of USAC Information in the possession or under the control of Contractor or its employees or any subcontractors or their employees. Contractor shall not withhold any USAC Information as a means of resolving any dispute. To the extent that there is a dispute between Contractor and USAC, Contractor may make a copy of such USAC Information as is necessary and relevant to resolution of the dispute. Any such copies shall promptly be destroyed upon resolution of the dispute.

XVI. INFORMATION SECURITY

The Contractor shall establish and maintain safeguards to protect the confidentiality, integrity, and restricted availability of Confidential Information, including any PII, in its possession according to NIST, FISMA requirements, and the Office of Management and Budget ("OMB") requirements. This includes all information that is sent to and received from USAC and USAC Stakeholders. The Contractor and its subcontractors shall ensure that their respective local area networks, servers, and personal computers are secure from unauthorized access from within or outside their respective organizations. The Contractor shall not store or otherwise maintain any USAC Confidential Information in the Cloud, or back-up and store USAC's Confidential Information without first obtaining USAC's written consent.

XVII. MALICIOUS SOFTWARE

Contractor represents and warrants that it shall use its best efforts to prevent the introduction into USAC's network, software or systems ("USAC IT Systems") of any Software, program, routine, device, or other undisclosed feature that is designed to delete, disable, deactivate, interfere with or otherwise harm USAC's IT Systems or Data, or that is intended to provide unauthorized access or modifications ("Malicious Software"). Contractor agrees that if it introduces, or allows the introduction of Malicious Software into USAC's IT Systems

intentionally, negligently or by failure to maintain available safeguards, Contractor must, at no additional cost to USAC, eliminate, or reduce to the greatest extent possible, the effects of the Malicious Software, including restoring Data, and, if the Malicious Software causes a loss of operational efficiency, loss of data or other damages, to mitigate and restore such losses, and to indemnify USAC for any damages.

XVIII. FISMA PROVISIONS

The Contractor shall meet and comply with all USAC IT Security Policies and all applicable USAC, NIST, and FISMA requirements and other Government-wide laws and regulations for the protection and security of information systems and data. Contractor's security and privacy controls must be assessed against the same NIST criteria and standards (specifically NIST SP 800-53, rev. 4, or the latest version) as if they were a government-owned or-operated system, and comply with all FISMA requirements.

Safeguarding of Covered Contractor Information Systems:

USAC's data security strategy includes the requirement to ensure the security of data protection controls regardless of the location or the party responsible for those controls. As a Contractor, you serve a vital role to achieve this goal. Contractor shall apply the following minimum safeguarding requirements and procedures from NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" to protect covered Contractor information systems and USAC Data. USAC may require a written response that may be an attestation of compliance, a submission of supporting document, or both. If USAC requests a written response, Contractor is required to submit an electronic copy of the document(s) confirming compliance within 10 calendar days. If there are any requirements that are out of scope or that cannot be complied with, those requirements must be fully explained with a business justification.

The Contractor shall apply the following minimum safeguarding requirements and procedures to protect covered Contractor information systems. Requirements and procedures for safeguarding of covered Contractor information systems shall include, at a minimum, the following security controls:

1. Limit information system access to only authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2. Limit information system access to only the types of transactions and functions that authorized users are permitted to execute.
3. Verify and control/limit connections to and use of external information systems.
4. Control information posted or processed on publicly accessible information systems.
5. Identify information system users, processes acting on behalf of users, or devices.

6. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
7. Sanitize or destroy information system media containing USAC Information before disposal or release for reuse.
8. Limit physical access to organizational information systems, equipment, and the respective operating environments to only authorized individuals.
9. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
10. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
11. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
12. Identify, report, and correct information and information system flaws in a timely manner.
13. Provide protection from malicious code at appropriate locations within organizational information systems.
14. Update malicious code protection mechanisms when new releases are available.
15. Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

XX. TECHNOLOGY CONSIDERATIONS

For RFIs, RFPs, and/or contracts involving the acquisition of Commercial off-the-shelf (COTS) software:

Commercial off-the-shelf (COTS) or Software as a Service (SaaS) software deployed in the cloud or on USAC's on-premise infrastructure must satisfy the following requirements:

- The product must be able to utilize USAC's instance of OKTA's Identity and Access Management software for user authentication.
- OKTA is a cloud-based Identity and Access Management product used by USAC.
- Any USAC data stored in a COTS/SaaS product database must be easily accessed by USAC via standard web services or another standard access mechanism

For RFIs, RFPs, and/or contracts involving the development of custom software for Universal Service Fund (USF) systems (Lifeline, High Cost, Rural Healthcare, Schools and Libraries, Contributors):

Custom software developed for Universal Service Fund programs (Lifeline, High Cost, Rural Health Care, Schools and Libraries) shall reuse the USAC Technical Stack unless the contractor demonstrates that those components are unable to meet the requirements. Key components of USAC's Technical Stack include the following:

- Java programming language
- OKTA (Identity and Access Management)
- Postgres (Relational Database Management System)
- Elastic Search, Logstash, Kibana
- Atlassian based tools (SDLC)
- Apache Tomcat (Application Servers)
- Red Hat Enterprise Linux
- Business Intelligence, Reporting, Geographical Information System, and Data Warehouse tools

Further details of USAC's technical stack will be provided during the down-selection process.

XXI. PROPRIETARY RIGHTS

Contractor agrees that all Data, Software, Deliverables, reports or other materials (collectively "Materials") developed or conceived by Contractor and/or documented by Contractor in the performance of the Contract, as well as all modifications and improvements thereto and all other designs, discoveries and inventions, are USAC property and shall be deemed USAC Information pursuant to Section XV above and works made-for-hire for USAC within the meaning of the copyright laws of the United States. Accordingly, USAC shall be the sole and exclusive owner for all purposes for the use, distribution, exhibition, advertising and exploitation of such Materials or any part of them in any way and in all media and by all means throughout the universe in perpetuity.

The Contractor shall not, without the prior written permission of the USAC Procurement Office, incorporate in Data delivered under the Contract any Data not first produced in the performance of the Contract unless the Contractor: (1) identifies the Data; and (2) grants to USAC, or acquires on USAC's behalf, a license of the same scope as set forth earlier in this Section XIX.

XXII. RESPONSIBILITY FOR CONTRACTOR PERSONNEL

Contractor personnel working on USAC premises are required to sign and agree to the terms of a Visitor Form provided by USAC. Contractor is responsible for any actions of its personnel, including any actions that violate law, are negligent or that constitute a breach of the Visitor Form and/or the Contract.

Security Briefings. Before receiving access to IT resources under the Contract, Contractor personnel must provide security training to its own employees. USAC will review and approve Contractor's security training materials and verify that training certifications and records will be provided upon request, if requested during the annual FISMA audit. If Contractor employees will be in USAC offices or have access to USAC IT systems, pursuant to NIST, Contractor shall conduct background checks on its employees and provide evidence of the background checks to USAC upon request. If Contractor employees will be in USAC offices or have access to USAC IT systems, background checks are required pursuant to NIST.

XXIII. RECORD RETENTION

During the term of the Contract and for three (3) years following final payment, the Contractor shall maintain and make available at its offices at all reasonable times, the records, materials, and other evidence relating to the Contract for examination, audit, or reproduction.

XXIV. KEY PERSONNEL

All Contractor employees assigned to the positions identified in Section B.IX are key personnel. The key personnel assigned to the Contract must remain in their respective positions throughout the term of the Contract, as applicable. USAC may terminate all or a part of the Contract if the Contractor changes the position, role, or time commitment of key personnel, or removes key personnel from the Contract, without USAC's prior written approval. USAC may grant approval for changes in staffing of key personnel if it determines in its sole discretion, that:

- changes to, or removal of, key personnel is necessary due to extraordinary circumstances (e.g., a key personnel's illness, death, termination of employment, or absence due to family leave), and

- the Contractor has resources (e.g., replacement personnel) with the requisite skills, qualifications and availability to perform the role and duties of the outgoing personnel.

Replacement personnel are considered key personnel and this Section XXII shall apply to their placement on and removal from the Contract.

XXV. INSURANCE

At its own expense, Contractor shall maintain sufficient insurance in amounts required by law or appropriate for the industry, whichever is greater, to protect and compensate USAC from all risks and damages/injuries that may arise under the Contract, including as appropriate, public and commercial general liability, personal injury, property damage and employer's liability and worker's compensation insurance. Contractor shall produce evidence of such insurance upon request by USAC. Contractor shall provide written notice thirty (30) days prior to USAC in the event of cancellation of or material change in the policy.

XXVI. CONFLICTS OF INTEREST

It is essential that any Contractor providing Services or Deliverables in support of USAC's administration of the USF maintain the same neutrality, both in fact and in appearance, and avoid any conflict of interest or even the appearance of a conflict of interest. For example, to the extent that Contractor, or any of its principals, has client, membership, financial and/or any other material affiliation with entities that participate in the federal USF in any respect, there may be actual, potential and/or apparent conflict(s) of interest. Contractor shall promptly notify USAC, with a copy to USAC's General Counsel, in writing of any actual or potential conflicts of interest involving Contractor, or any circumstances that give rise to the appearance of a conflict of interest, and the means by which Contractor proposes to avoid, neutralize, or mitigate such conflicts. Contractor shall also notify USAC of any conflicts Contractor has with USAC vendors. Failure to provide adequate means to avoid, neutralize or mitigate any conflict of interest may be the basis for termination of the Contract. By its execution hereof, the Contractor represents and certifies that it has not paid or promised to pay a gratuity, or offered current or future employment or consultancy, to any USAC or governmental employee in connection with the award. In order to maintain the required neutrality, Contractor must not advocate any policy positions with respect to the Programs or the USF during the term of the Contract. Neither the Contractor nor its subcontractors shall issue any public statement relating to or in any way disclosing any aspect of the Contract without the prior written consent of USAC.

XXVII. INVALIDITY OF ANY PROVISION

It is the intent of the Parties that the provisions of the Contract will be enforced to the fullest extent permissible, but that the unenforceability of any provision will not render unenforceable or impair the remainder of the Contract, which will be deemed amended, to delete or modify, as necessary, the invalid or unenforceable provisions. The Parties further agree to negotiate replacement provisions for any unenforceable term that are as close as possible to the original term and to change such original term only to the extent necessary to render the same valid and enforceable.

XXVIII. WAIVER

Any waiver by either party of a breach of any provision of the Contract shall not operate or be construed as a waiver of any subsequent breach by either party.

XXIX SEVERABILITY

The invalidity or unenforceability of any provisions of the Contract shall not affect the validity or enforceability of any other provision of the Contract, which shall remain in full force and effect.

XXX. CHOICE OF LAW / CONSENT TO JURISDICTION

The Contract shall be governed by and construed in accordance with the laws of the District of Columbia (the term "laws" is to be construed as broadly as possible to include case law, statutes, regulations, orders, etc.) without regard to any otherwise applicable principle of conflicts of laws. Contractor agrees that all actions or proceedings arising in connection with the Contract shall be litigated exclusively in the State and, if applicable, Federal courts located in the District of Columbia ("Courts"). This choice of venue is intended to be mandatory and the parties' waive any right to assert forum non conveniens or similar objection to venue. Each party hereby consents to in personam jurisdiction in the Courts. Contractor must submit all claims or other disputes to the Contracting Officer for informal resolution prior to initiating any action in the Courts and must work with USAC in good faith to resolve any disputed issues. A dispute over payment or performance, whether informal or in the Courts, shall not relieve Contractor of its obligation to continue performance of the Contract and Contractor shall proceed diligently with performance during any dispute over performance or payment.

XXXI. USAC AND APPLICABLE LAWS

USAC is not a Federal agency, a government corporation, a government controlled corporation or other establishment in the Executive Branch of the United States Government. USAC is not a contractor to the Federal Government and the Contract is not a subcontract under a federal prime contract. USAC conducts its procurements in accordance with the terms of a Memorandum of Understanding with the FCC, which requires USAC and its Contractors to adhere to certain procurement-related provisions of the Code of Federal Regulations, 2 C.F.R. §§ 200.318-321, 200-323, 200.325-326 and App. II to C.F.R. Part 200 (collectively "Procurement Regulations"). The Contractor shall comply with the procurement standards and all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under the Contract.

XXXII. RIGHTS IN THE EVENT OF BANKRUPTCY

All licenses or other rights granted under or pursuant to the Contract are, and shall otherwise be deemed to be, for purposes of Section 365(n) of the United States Bankruptcy Code, or any replacement provision therefore (the "Code"), licenses to rights to "intellectual property" as defined in the Code. The Parties agree that USAC, as licensee of such rights under this Contractor, shall retain and may fully exercise all of its rights and elections under the Code. The Parties further agree that, in the event of the commencement of bankruptcy proceedings by or against Contractor under the Code, USAC shall be entitled to retain all of its rights under the Contract and shall not, as a result of such proceedings, forfeit its rights to any Material, license, Software, Data or works made for hire.

XXXIII. NON EXCLUSIVITY / INDEPENDENT CONTRACTOR

Nothing herein shall be deemed to preclude USAC from retaining the services of other persons or entities undertaking the same or similar functions as those undertaken by the Contractor hereunder or from independently developing or acquiring goods or services that are similar to, or competitive with, the goods or services, as the case may be, contemplated under the Contract.

Contractor acknowledges and agrees that it is an independent contractor to USAC and Contractor's key personnel, employees, representatives, directors, officers, subcontractors and agents are not employees of USAC. USAC will not withhold or contribute to Social Security, workers' compensation, federal or state income tax, unemployment compensation or other employee benefit programs on behalf of Contractor or Contractor personnel. Contractor shall indemnify and hold USAC harmless against any and all loss, liability, cost and expense (including attorneys' fees) incurred by USAC as a result of USAC not withholding or making such payments. Neither Contractor nor any of Contractor's personnel are entitled to participate in any of the employee benefit plans of, or otherwise obtain any employee benefits from, USAC. USAC has no obligation to make any payments to Contractor's key personnel, employees, representatives, directors, officers, subcontractors and agents. Contractor shall not hold herself/himself out as an employee of USAC and Contractor has no authority to bind USAC except as expressly permitted hereunder.

XXXIV. TEMPORARY EXTENSION OF SERVICES

USAC may require continued performance of any Contract services within the limits and at the rates specified in the Contract. USAC may extend the services more than once, but the total extension of performance hereunder shall not exceed six (6) months. The USAC Procurement representative may exercise an option to extend by written notice to the Contractor within ten (10) days prior to expiration of the then current term.

XXXV. NOTICES

All notices, consent, approval or other communications required or authorized by the Contract shall be given in writing and shall be:

(a) personally delivered,
(b) mailed by registered or certified mail (return receipt requested) postage prepaid,
(c) sent by overnight delivery service (with a receipt for delivery), or
(d) sent by electronic mail with a confirmation of receipt returned by recipient's electronic mail server to such party at the following address:

If to USAC:
Vice President of Procurement and Strategic Sourcing, Universal Service Administrative Co.
700 12th Street, NW, Suite 900
Washington, DC 20005
Email: To the designated USAC Contract Officer for this procurement, with a copy to usacprocurement@usac.org.

If to Contractor: To the address or email set forth in the Contractor's proposal in response to the Solicitation.

XXXVI. SURVIVAL

All provisions that logically should survive the expiration or termination of the Contract shall remain in full force and effect after expiration or early termination of the term of the Contract. Without limitation, all provisions relating to return of USAC information, confidentiality obligations, proprietary rights, and indemnification obligations shall survive the expiration or termination of the Contract.

XXXVII. EXECUTION / AUTHORITY

The Contract may be executed by the parties hereto on any number of separate counterparts and counterparts taken together shall be deemed to constitute one and the same instrument. A signature sent via facsimile or portable document format (PDF) shall be as effective as if it was an original signature. Each person signing the Contract represents and warrants that they are duly authorized to sign the Contract on behalf of their respective party and that their signature binds their party to all provisions hereof.

XXXVIII. INDEMNITY

Contractor shall defend, indemnify and hold harmless USAC from and against, any costs, liabilities, damages or expenses (including reasonable attorneys' fees) arising out of or relating to: (1) claims for personal injuries, death or damage to tangible personal or real property to the

extent proximately caused by the negligent acts or negligent omissions of Contractor or its employees, agents, consultants, or Subcontractors in connection with this Contract; and (2) claims of any nature whatsoever to the extent caused by the violation of Contract terms, negligence, illegal or intentional wrongful acts or omissions of Contractor or its employees, agents, consultants, or Subcontractors in connection with the performance of the Services.

SECTION D:
Attachments

Attachment List:

- Attachment 1: Bid Sheet

- Attachment 2: Resumes/Biographies for Selected Key and Non-Key Personnel

SECTION E:
Instructions and Evaluation Criteria

I. GENERAL

A. CONTRACT TERMS AND CONDITIONS

The Contract awarded as a result of this RFP will be governed by, and subject to, the requirements, Terms and Conditions set forth in RFP sections A, B, C, and D and any attachments listed in section D (hereafter collectively referred to as the "Terms and Conditions"). Offeror's submission of a proposal constitutes its agreement to the Terms and Conditions and their precedence over any other terms, requirements, or conditions proposed by Offeror.

The Offeror's proposal shall identify deviations from, or revisions, exceptions or additional terms (collectively "exceptions") to the Terms and Conditions, but only if such exceptions are clearly identified in a separate **Attachment B** to Volume II, "Exceptions to RFP Terms." Proposals that include material exceptions to the Terms and Conditions may be considered unacceptable and render Offeror ineligible for award unless the Offeror withdraws or modifies any unacceptable exceptions prior to USAC's selection of the successful Offeror for award. USAC will only consider changes or additions to the RFP Terms and conditions that are included in Offeror's proposal. Exceptions to the Terms and Conditions will only be accepted during proposal submission and will not be reviewed or considered during the time of Contract negotiation. After selection of the awardee, USAC will not consider or negotiate any exceptions to the Terms and Conditions.

B. PERIOD FOR ACCEPTANCE OF OFFERS

The Offeror agrees to hold the fixed service category rates in its offer firm for 120 calendar days from the date specified for receipt of offers, unless another time period is specified in an addendum to the solicitation.

Proposals must:

- Concisely address USAC's requirements, as set forth in Section B.VIII. Performance Requirements and Scope of Work (Section B), and should not contain a significant amount of corporate boilerplate marketing information.
- Be submitted to USAC Procurement Department, no later than 11:00 AM ET on **May 6, 2019** (Proposal Due Date).

- Be submitted in the form of one electronic copy submitted to rfp@usac.org. The subject line for all email communication related to this solicitation should **only** state the Solicitation Number, IT-19-041, of this RFP.

C. ANTICIPATED PROPOSAL SCHEDULE

DATE	EVENT
4/23/2019	RFP Released
4/25/2019	Questions Due to USAC by 11:00 AM ET at rfp@usac.org
4/26/2019	Answers posted by USAC
5/6/2019	Proposal Due to USAC by 11:00 AM ET at rfp@usac.org
5/14/2019	Potential date for oral discussions, if necessary
5/15/2019	Final Proposal Revisions due
5/31/2019	Anticipated Award Date
6/3/2019	Work Begins

To be timely, Offeror's proposal must be received by USAC by the Proposal Due Date at the email address specified above. Any offer, modification, revision, or withdrawal of an offer received at the USAC office designated in the solicitation after the Proposal Due Date and Time is "late" and will not be considered by USAC, unless USAC determines, in its sole discretion, that (1) circumstances beyond the control of Offeror prevented timely submission, (2) consideration of the offer is in the best interest of USAC, or (3) the offer is the only proposal received by USAC.

D. AMEND, REVISE OR CANCEL RFP

USAC reserves the right to amend, revise or cancel this RFP at any time at the sole discretion of USAC and no legal or other obligations are assumed by USAC by virtue of the issuance of this RFP, including payment of any proposal costs or expenses, or any commitment to procure the services sought herein.

II. CONTRACT AWARD

USAC intends to evaluate offers and make a single award. USAC may reject any or all offers if such action is in the public's or USAC's interest; accept other than the lowest offers; and waive informalities and minor irregularities in offers received.

III. IDENTIFICATION OF CONFIDENTIAL INFORMATION

The proposal shall clearly and conspicuously identify information contained in the proposal that the Offeror contends is Confidential Information. *See* Section C.XIV.

IV. PROPOSAL VOLUMES COVER PAGE

Each volume of Offeror's proposal must contain a cover page. On the cover page, please include:

- The name of the Offeror's organization,
- The Offeror's contact name and title,
- The Offeror's contact information (address, telephone number, email address, website address),
- The Offeror's data universal numbering system ("DUNS") number,
- The date of submittal,
- A statement verifying the proposal is valid for a period of 120 days, and
- The signature of a duly authorized Offeror's representative.

V. PROPOSAL CONTENT

Each proposal shall be comprised of the following four (4) volumes:

A. CORPORATE INFORMATION (VOLUME I)

This volume must include:

1. A cover page, as outlined above.

2. An executive summary summarizing all key features of the proposal, including the identification of any subcontractors and affiliated individuals or firms that will assist the Offeror in performing the Contract.

3. Pricing information should not appear in Volume I.

4. A statement regarding any known conflicts of interest.

    a. USAC procurements are conducted with complete impartiality and with no preferential treatment. USAC procurements require the highest degree of public trust and an impeccable standard of conduct. Offerors must strictly avoid any conflict of interest or even the appearance of a conflict of interest, unless USAC has otherwise approved an acceptable mitigation plan.

    b. Offerors must identify any actual or potential conflicts of interest including current USAC vendors involving the Offeror or any proposed subcontractor, or any

circumstances that give rise to the appearance of a conflict of interest, and the means by which it proposes to avoid, neutralize, or mitigate such conflicts. Offerors shall identify such conflicts or potential conflicts or appearance issues to USAC and provide detailed information regarding the nature of the conflict. Examples of potential conflicts include, but are not limited to: (1) any ownership, control or other business or contractual relationship(s), including employment relationships, between the Offeror (or proposed subcontractor) and any USF Stakeholder; (2) an Offeror has a direct personal or familial relationship with a USAC or FCC employee; (3) a former employee of USAC or FCC who had access to confidential procurement-related information works for the Offeror; (4) a USAC or FCC employee receives any type of compensation from the Offeror, or has an agreement to receive such compensation in the future; (5) Offeror has communications with a USAC or FCC employee regarding future employment following the issuance of the RFP for this procurement; (6) any employment or consultation arrangement involving USAC or FCC employees and the Offeror or any proposed subcontractor; and (7) any ownership or control interest in the Offeror or any proposed subcontractor that is held by an FCC or USAC employee. Offerors must also identify any participation by the Offeror, or any proposed subcontractor(s) or personnel associated with the Offeror, in any of the universal service programs. The requirement in this Section E.V.A applies at all times until Contract execution.

c. Offerors shall propose specific and detailed measures to avoid, neutralize, or mitigate actual, potential and/or apparent conflicts of interest raised by the affiliations and services described above. If USAC determines that Offeror's proposed mitigation plan does not adequately avoid, neutralize or mitigate any actual or potential conflict of interest, or the appearance of a conflict of interest, Offeror will not be eligible for award of a contract.

B. TECHNICAL (VOLUME II)

This volume must include:

1. A cover page, as outlined above.

2. A summary detailing Offeror's experience providing security control assessments in the capacity described in Section B of this RFP.

3. An in-depth discussion of Offeror's technical approach to providing the services listed in Section B.VI., along with a clear statement of whether or not the Offeror's performance of the Contract will comply with all requirements, Terms and Conditions

set forth in the RFP. Offerors must submit a detailed response to this RFP. The Offeror must clearly state whether it will comply with all requirements and Terms and Conditions set forth in the RFP, and provide detailed information about how it will fulfill the requirements of the RFP. Any deviations from, or exceptions to, the requirements or Terms or Conditions contained in this RFP must be clearly identified in an Attachment B to Volume II.

> Note: Offers that include material deviations from, or take material exceptions to, RFP requirements, Terms or Conditions will be evaluated as technically unacceptable and will be ineligible for award unless USAC subsequently amends the RFP to modify the requirements or, if discussions will be held, decides to address the deviations/exceptions during discussions and thereby resolves the deviations/exceptions are thereby resolved.

4. Technical proposals that merely repeat the requirements set forth in the RFP and state that Contractor "will perform the statement of work" or similar verbiage will be considered technically unacceptable and will not receive further consideration. USAC is interested only in proposals that demonstrate the Contractor's expertise in performing engagements of this type as illustrated by the Offeror's description of how it proposes to perform the requirements set forth in this RFP.

5. Capabilities. Describe Offeror's capabilities for performing the Contract, including personnel resources and management capabilities. If applicable, describe how subcontractors or partners are used and how rates are determined when using subcontractors. Provide a list of firms, if any, that will be used.

6. Timeline. Offerors shall describe in detail their process for conducting activities to manage the SCA, including how the Offeror intends to staff and complete related activities. Offerors shall describe in detail their plan for completing the services as identified in Section B.V and Section B.VI. in a time allotted. If Offeror currently has staff or personnel who meet the qualifications for the services identified in Section B.V and Section B.VI who are available for assignment under an awarded contract, please provide a resume (not to exceed two (2) pages per resume) that includes their educational background, specific job and related experience, and the specific position(s) for which they are available on the Contract.

7. Experience. Describe your firm's experience with providing SCA services as detailed in Section B of this RFP. Provide examples of projects and personnel to include project scope, size, and complexity, and types of positions with length of assignments.

8. Key Personnel. Identify by name all key personnel. Describe the technical knowledge and experience of proposed personnel in the requested services with respect to, but not limited to, experience and qualifications including depth of knowledge, expertise and number of years. It is preferred that the Provide two (2) clients in which the proposed held a similar position. Indicate any other personnel that will be assigned to USAC and his/her role on the contract. Provide a brief summary of each of these professional staff members' qualifications to include education and all relevant experience.

    a. Contractor shall provide the resumes/biographies of three (3) sample executive peer advisors.

    b. Submit resumes/biographies for all key personnel, as an attachment (**Attachment 3**) to the technical volume, no longer than two (2) pages in length per resume.

    c. If Contractor, at the time of proposal and prior to the award of the Contract, has information that any such key personnel anticipate terminating his or her employment or affiliation with Contractor, Contractor shall identify such personnel and include the expected termination date in the proposal.

C. PAST PERFORMANCE EVALUATION (VOLUME III)

This volume must include:

1. A cover page, as outlined above.

2. A list of three (3) current or recently completed contracts (no older than 3 years from the date of the solicitation) similar in scope to those required by this solicitation. Each entry on the list **must** contain:

    a. the client's name;
    b. the project title;
    c. the period of performance;
    d. the Contract number;
    e. the Contract value;
    f. a primary point of contact (including the telephone number and email address for each point of contact, if available);
    g. a back-up point of contact.

If a back-up point of contact is not available, please explain how USAC may contact the client in the event the primary point of contact fails to respond.

a. For each past performance, provide a description of the relevant performance and the name and telephone number for USAC to contact for past performance information for each project discussed. A past performance description will consist of:

(i) an overview of the engagement;
(ii) a description of the scope of work performed;
(iii) its relevance to this effort;
(iv) the results achieved.

This is the time to identify any unique characteristics of the project, problems encountered, and corrective actions taken. Each overview shall not exceed one (1) page.

b. USAC will attempt to contact past performance references identified in the proposal for confirmation of the information contained in the proposal and/or will transmit a past performance questionnaire to the contacts identified in the Offeror's proposals. Although USAC will follow-up with the contacts, the Offeror, not USAC, is responsible for ensuring that the questionnaire is completed and returned by the specified date in USAC's transmittal. If USAC is unable to reach or obtain a reference for the project, USAC may not consider the Contract in an evaluation of past performance.

D. PRICE (VOLUME IV)

This volume must include:

1. A cover page, as outlined above.

2. Completed pricing information in **Attachment 1: Bid Sheet**.

   a. The fixed Security Controls Assessment activities prices should be *fully burdened* and must include wages, overhead, general and administrative expenses, taxes and profit.

E. PAGE COUNT LIMITS

Page count, for each Volume including the Cover page, may not exceed the below:

1. Volume I – Corporate Information; may not exceed three (3) pages, including Cover page.

2. Volume II – Technical; may not exceed fifteen (15) pages including Cover page; however excluding **Attachment 2** (Resumes)

3. Volume III – Past Performance Information; may not exceed four (4) pages, including Cover page.

4. Volume IV – Price; may not exceed two (2) pages, including Cover page.

Any proposals received exceeding the page count, will be considered technically unacceptable and may not receive further consideration.

VI. EVALUATION

A. EVALUATION FACTORS

USAC will award a single contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to USAC, price and other factors considered. The following factors, which are listed in descending order of importance, shall be used to compare offers and select the awardee – technical, past performance, and price. When combined, the technical and past performance factors are significantly more important than price.

1. **Technical:** The technical sub-factors listed below in descending order of importance:

    a. Technical Approach
    b. Timeline
    c. Capabilities
    d. Experience
    e. Key Personnel

2. **Past Performance**: Past performance information will be evaluated to assess the risks associated with an Offeror's performance of this effort, considering the relevance, how recent the project is (no older than 3 years from the date of the solicitation), and quality of the Offeror's past performance on past or current contracts for the same or similar services. Past performances The Offeror's past performance will be evaluated based on the Offeror's discussion of its past performance for similar efforts, information obtained

from past performance references (including detailed references for the Offeror's proposed teaming partner(s) and/or subcontractor(s), as applicable) and information that may be obtained from any other sources (including government databases and contracts listed in the Offeror's proposal that are not identified as references).

3. **Price Evaluation**: USAC will evaluate price based on the firm fixed price, listed in the Bid Sheet.Price is the least important evaluation factor and USAC may not necessarily award a Contract to the lowest priced Offeror. USAC further recognizes that the size of a company, its name-recognition, geographical offerings and the expertise/experience of staff impacts the price of the service category rates offered by the firms, thus making comparisons of differently situated firms less meaningful. Therefore, when considering rates, USAC will use the rates of similarly situated companies for reasonableness and comparison purposes. Price may become a more important selection factor if the ratings for the non-price factors are the same or very close to the same. In addition to considering the total prices of the Offerors when making the award, USAC will also evaluate whether the proposed prices are realistic (i.e., reasonably sufficient to perform the requirements) and reasonable. Proposals containing prices that are determined to be unrealistic or unreasonable will not be considered for award.

B. DOWN-SELECT PROCESS

USAC may determine that the number of proposals received in response to this RFP are too numerous to efficiently conduct a full evaluation of all evaluation factors prior to establishing a competitive range. In such case, USAC may conduct a down-select process to eliminate Offerors, prior to discussions, from further consideration based on a comparative analysis of Offerors proposals, with primary focus on the price proposal, but USAC may, in its sole discretion, consider other factors such as failure to follow instructions as provided, quality of proposal, technical capabilities and past performance. Proposals that include proposed prices that are significantly higher than the median proposed price for all Offerors may be excluded from the competition without evaluation under the other evaluation factors. Proposals that contain prices that are unrealistically low in terms of sufficiency to perform the Contract may also be excluded from the competition.

C. RESPONSIBILITY DETERMINATION

USAC will only award a contract to a responsible Offeror. USAC will make a responsibility determination based on any available information, including information submitted in an Offeror's proposal. In making a responsibility determination, USAC will consider whether:

1. the Offeror has sufficient resources to perform the Contract;

2. the Offeror has a satisfactory record of performance, integrity and business ethics;

3. the Offeror has the accounting systems and internal controls, quality assurance processes and organizational structure and experience necessary to assure that contract work will be properly performed and accurately invoiced;

4. the Offeror has the facilities, technical and personnel resources required to perform the Contract; and

5. the Offeror is not excluded from Government contracting, as listed on the excluded parties list in https://www.sam.gov.