Mock Task Order Request for Proposal #1:
Security Controls Assessment
Professional Services RFP – FISMA Compliance Consulting Services

CAPITALIZED TERMS USED BUT NOT DEFINED IN THIS TORP HAVE THE MEANING SET FORTH IN PROFESSIONAL SERVICES CONTRACT # USAC-20-015 (THE "CONTRACT"). AND THIS TORP IS ISSUED PURSUANT TO AND UNDER THE TERMS AND CONDITIONS SET FORTH IN THE CONTRACT.

I. TASK ORDER TYPE

This is a single award, firm fixed price task order (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.

II. PURPOSE

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, including 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

III. 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.

IV. PURPOSE OF THIS TORP

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.

V. 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.

VI. TASK ORDER PERIOD OF PERFORMANCE

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.

VII. PLACE OF PERFORMANCE

Contractors shall perform Task Orders at either its own facilities or at USAC Headquarters. Occasional meetings may be conducted at USAC's Headquarters or at the FCC offices located at 445 12th Street SW, Washington, DC 20554. USAC shall provide appropriate office space and appropriate access to its computer network for duties performed at USAC Headquarters, if necessary. Contractors will be required to complete USAC's Visitor Form, USAC Visitor Form and wear a badge while on USAC premises.

VIII. TASK ORDER PROCESS

Attachment 1 Pricing. Fixed labor-hour rates for T&M must be fully burdened and include all wages, overhead, general and administrative expenses, taxes and profit, and individual laptop equipment and office software for each category of labor. Services for the T&M CLINS shall be performed on a T&M basis using the labor categories and fixed hourly rates set forth in Attachment

A. ***Task Order Ceiling Price.*** Each Task Order issued under the Contract will include a ceiling price (the "Task Order Ceiling Price"). USAC will not be obligated to pay Contractor any amount in excess of the Task Order Ceiling Price, and Contractor shall not be obligated to continue performance if to do so would exceed the Task Order Ceiling Price, unless and until USAC notifies Contractor in writing that the Task Order Ceiling Price has been increased and specifies in the notice a revised ceiling price that shall apply to the Task Order.

B. ***Steps for each Task Order***

1. Issuance of Task Orders. USAC will issue Task Orders in accordance with the procedures set forth below. As specified in each Task Order issued under the Contract, Contractor shall provide experienced personnel who are capable of performing the tasks described in, and who meet the qualifications listed under, the Key Personnel set forth below.

2. Work Schedule. Unless otherwise specified in a Task Order, Contractor personnel assigned to a Task Order shall maintain a work schedule consistent with USAC normal business hours and work practices. Contractor personnel are expected to comply with all of USAC's rules pertaining to conduct in the workplace. Any change in Contractor personnel must be approved, in writing, by the USAC Procurement department and reflected in the Task Order. Contractor personnel are not employees of USAC.

3. Invoicing and Reporting Instructions. Each Task Order will outline the invoicing and reporting instructions required specifically for that project.

4. Task Order Proposals. Contractor shall perform the following steps which are necessary for the Task Order award. Contractor shall submit one proposal in response to each TORP. See Attachment 1, Mock TORP. Each Contractor proposal in response to a TORP must include the following information:

   a. *Basic Information*. A cover page which includes:
      1. The name of Contractor's organization;
      2. Offeror's contact name;
      3. Offeror's contact information (address, telephone number, email address, website address);
      4. Offeror's DUNS number;
      5. The date of submission;
      6. A statement verifying the proposal is valid for a period of 120 days; and
      7. The signature of a duly authorized Offeror representative.

b. *Production Schedule*. A detailed and comprehensive production schedule that includes a proposed schedule and approach for managing and providing the Services and Deliverables required by the TORP. Contractor should also outline any deviations from the TORP.

c. *Pricing*. A total hourly breakdown of each Contractor proposed staff.

d. *Ceiling Price*. A proposed Task Order ceiling price for the TORP, as well as a justification.

C. ***Task Order Proposal Review***. USAC will review Contractor's proposal to this TORP, provide feedback if any adjustments or negotiations are required, and subsequently award the Task Order.

IX. SCOPE OF SERVICES AND DELIVERABLES

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.

A. PERFORMANCE REQUIREMENTS

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.

B. 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 Timetable

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
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

RMF	Deliverable	Frequency	Medium/Format	Deliver To
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
2020 Milestones		
3	ISCM	TBD
1	ISCM	TBD
2	ISCM	TBD
2	ATO	TBD
2021 Milestones		
3	ISCM	TBD
2	ISCM	TBD
2	ISCM	TBD
1	ATO	TBD
2	ATO	TBD
2022 Milestones		
3	ISCM	TBD
2	ISCM	TBD
2	ISCM	TBD
1	ISCM	TBD
2	ISCM	TBD
2023 Milestones		
3	ISCM	TBD
2	ISCM	TBD
2	ISCM	TBD
1	ISCM	TBD
2	ISCM	TBD
2024 Milestones		
3	ISCM	TBD

2	ISCM	TBD
2	ISCM	TBD
1	ISCM	TBD
2	ISCM	TBD

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;

X. KEY PERSONNEL

A list, by name, of all Key Personnel, along with the labor category they will fill. For each Key Personnel, Contractor shall provide a biography that includes his/her educational background, skill-set, job and related experience, a list of specific efforts he/she has supported, and references. Contractor shall provide a Relationship Manager ("RM") who shall ensure the completion and delivery of the Task Order and serve as a single point of contact for the day-to-day management of the Task Order.

All pricing information for the TORP shall be based on Contractor's Attachment 1: Bid Sheet to the Contract.

XI. KEY PERSONNEL & LABOR CATEGORIES

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)

XII. INVOICES

Where to Submit Invoices. Contractor shall submit invoices through the USAC Coupa Supplier Portal ("CSP") method or via the Supplier Actionable Notification ("SAN") method. The CSP method will require Contractor to register and create an account for the CSP. An invitation link to the CSP may be obtained by emailing CoupaHelp@usac.org. The SAN method will require Contractor to invoice USAC directly from the purchase order ("PO") sent by USAC via email. For the SAN method, the USAC email will contain a notification with action buttons which will allow Contractor to create an invoice, add a comment, and acknowledge the receipt of the PO. For assistance on all Coupa related billing questions, Contractor may email CoupaHelp@usac.org. For assistance on all non-Coupa related billing questions, Contractor may email accounting@usac.org.

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.

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.

XIII. COMMUNICATION

Contractor shall be reasonably available and accessible via email or telephone during USAC's normal business hours, which are Monday through Friday (9:00AM-6:00PM ET). When necessary, communication may be made outside of these hours to ensure the progress of the Contract is not impeded.

XIV. MEETINGS

During performance of the Task Order, Contractor personnel shall communicate on a regular basis with USAC staff, and, as requested by USAC's COR or CA, attend status meetings with USAC staff to discuss project status and progress, impediments, and audit findings. Status meetings will be held by either teleconference or in person. Status reports may be used as the basis of the status meeting discussions.

XV. TRAVEL

Contractor staff may be required to travel to USAC to perform Services under the Task Order. Contractors may invoice for up to 10% of the total Task Order value in travel expenses, provided Contractor complies with the terms and conditions of the USAC travel policies. All Contractor travel costs should be included in the Contractor's proposed Task Order Ceiling Price.

XVI. TASK ORDER PROPOSAL SUBMISSION INSTRUCTIONS

All responses, to this TORP, are due no later than **11:00 AM ET, March 12, 2020, 2020**. Responses received after this date and time or do not follow the task order submission instructions, may not be considered for review.

Responses should be prepared simply and economically, and provide a straightforward and concise explanation of the information requested. Emphasis should be on completeness and clarity.

Please submit one (1) electronic copy (PDF) of your response to Becca Wray at rfp@usac.org. All submissions must include "Response to Task Order #01 – Security Controls Assessment" in the subject line.

Please note: all electronic submissions must be limited to a maximum size of 25 GB.