USAC Solicitation for Information Security Program Compliance Support

Revised

SOLICITATION INFORMATION:

Method of Solicitation:	Request for Proposal (RFP)
Award Effective Date:	TBD
Contract Period of Performance:	One base year plus 3 option years
Solicitation Number:	IT-22-012
Solicitation Issue Date:	February 4, 2022
Question Due Date	February 14, 2022 by 11:00 AM ET
Offer Due Date:	March 7, 2022 by 11:00 AM ET

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
Noor Jalal Senior Procurement Specialist P: 202-263-1616 E: noor.jalal@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

1. ABOUT USAC

Through its administration of the Universal Service Fund ("USF") programs on behalf of the Federal Communications Commission ("FCC"), Universal Service Administrative Company ("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 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, Audit and Assurance, 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 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.

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 has built the National Verifier, which includes the National Lifeline Eligibility Database to determine subscriber eligibility.

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 RHC 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.

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.

Additional information on USAC programs can be found at:
https://www.usac.org/about/universal-service/

2. PURPOSE OF THIS RFP

USAC is seeking a contractor to provide consulting and support services to act as an integral part of the Information Security Program Compliance team. The selected contractor ("Contractor") is expected to work directly with USAC staff in order to satisfy the objectives of the Information Security Program Compliance Support Contract.

The overall goal is to build and sustain a professional, enterprise information security program that protects all USAC data, information systems and assets, cradle-to-grave, through a combination of disciplined processes, people, and technologies.

3. Confidentiality

This RFP and any resultant contract is subject to the terms of the Confidentiality Agreement (attached hereto as Attachment 3) which must be executed by Offeror and submitted along with any proposal for this RFP.

SECTION B:
Requirements and Scope of Work

1. OVERVIEW

Contractor shall provide Information Security Program Compliance Support services for USAC. Contractor shall act as an integral part of the USAC organization driving successful outcomes required by USAC's Information Security program.

USAC's Information Security Program adheres to the Federal Information Security Management Act ("FISMA") / National Institute of Standards and Technology ("NIST") framework for information security. This framework has been applied to systems in production and new systems being developed that support the mission of the USF.

The USAC organizational characteristics with respect to Information Security, are as follows:

- Five (5) Customer-Facing business units that interact via web-based applications and application programming 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 premises. More recent systems are managed in third party vendor's cloud environments.

- The business support units (Human Resources, Internal Audit, General Counsel, and Information Technology) mostly have Commercial Off the Shelf ("COTS") based support systems that are configured to meet business unit requirements.

Contractor shall provide Information Security Program Compliance Support services to include:

a. Information System Security Officer ("ISSO") Support
    1. Baseline Assessment & Authorization ("A&A") Support
    2. Ongoing Security Authorization ("OSA") Program
    3. Information Security Policies, Procedures, and Standards Management
    4. IT Security Governance, Risk Management, and Compliance ("GRC") Tool Administration

b. Plans of Action and Milestones ("POA&M") and Vulnerability Management Program Support
    1. POA&M Management Program
    2. Vulnerability Management Program

c. IT Risk Management Program

d. Supply Chain Risk Management ("SCRM") Program

2. TYPE OF CONTRACT

The contract to be awarded pursuant to this RFP will be a firm fixed price single-award contract ("Contract"). The firm fixed price for the work (total project and all line items) is to be set forth in **Attachment 1** to the Contractor Response to the RFP. 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.

3. CONTRACT TERM

The term of this Contract shall be for a base period of one year (the "Initial Term") with three (3) one-year renewal options (each a "Optional Renewal Term"). The Initial Term, together with any exercised Optional Renewal Terms shall be defined as the "Contract Term". The duration of the Contract shall be the Contract Term unless extended by USAC or terminated sooner in accordance with the Contract. The Contract Term shall commence on the first day of the Contract Period of Performance as stated in the Solicitation Information (the "Effective Date") set forth in the Contract.

4. PLACE OF PERFORMANCE

A. All Services provided pursuant to the Contract must be performed within the United States. Contractor shall perform Services at its own facilities. ~~and at the locations of the selected carriers.~~ USAC may conduct occasional meetings or training at its headquarters located at 700 12th Street NW, Suite 900, Washington, DC 20005 ("USAC 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. Each Contractor personnel will be required to sign-in to Confluence at the USAC Receptionist Desk and wear a badge while on premises. Status update meetings, and other scheduled meetings, will be held virtually, except to the extent that USAC or the Contractor requires an in-person meeting.

B. Contract kick-off meeting, training, status calls, and other meetings will be held via conference calls using either a conference center or an internet accessed platform, or in person at USAC's Headquarters. The location of these Contract events will be at USAC's discretion.

C. Services requiring work at USAC Headquarters will include appropriate work space and appropriate access to USAC's computer network. USAC will provide laptop to all contract personnel. No additional hardware or software 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 containing personally identifiable information (PII).**

D. Status update meetings and other meetings may be held virtually, except to the extent that USAC or Contractor requires in-person presence. While attending USAC Headquarters for meetings or to conduct the assessment, 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.

5. COMPANY PROFILE

USAC is a not-for-profit Delaware corporation, which works under the oversight of the FCC. 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. The Contract awarded as a result of this RFP will not be a subcontract under a federal prime contract. USAC does, however, conduct its procurements in accordance with the terms of a Memorandum of Understanding with the FCC, which requires USAC to adhere to the following provisions from 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"). Further, USAC IT Systems that are used to administer the USF programs and USAC vendors that handle and manage USF data must be compliant with FISMA and NIST requirements as applicable to federal agencies.

6. USAC PROGRAM MANAGER AND CONTRACTS ADMINISTRATOR

The Program Manager ("PM") for the Contract is Davon Nasir, the USAC point of contact for overseeing the performance of services. USAC's Contracts Administrator ("CA") for the Contract is Hameed Khairkhwah, the USAC point of contact for contractual matters (e.g., proposal submissions, task order modifications and other matters not related to performance).

7. STATEMENT OF WORK

A. Objectives: To obtain contractor support that:

a. Provides a working and holistic understanding and knowledge of the Risk Management Framework ("RMF") as defined by National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53 (latest revision), Recommended Security Controls for Federal Information Systems and NIST SP 800-53A (latest revision), Guide for Assessing the Security Controls in Federal Information Systems;

b. Serves as the source of technical expertise with regards to maintaining and improving the USAC's RMF implementation;
c. Provides tactical production operations support for Assessment & Authorization ("A&A") activities including preparation for and support of independent third-party assessments for new systems, reauthorizations, and continuous monitoring;
d. Provides strategic guidance and recommendations for strategic planning and improvements to the systems/applications supported by the contractor;
e. Provides support to the USAC Chief Information Security Officer ("CISO") and Office of the CISO ("OCISO") at large; and
f. Develops, updates, and maintains management directives, security policies, security procedures, and standard operating procedures ("SOP") to support the Information Security Program as a whole, including both the IT Security Compliance and IT Security Operations components.

B. Information Security Program Compliance Support: Contractor shall provide the following services in support of the IT Security Compliance component within the Information Security Program and Business Process Outsource ("BPO") Third Party Vendors:

a. Information System Security Officer ("ISSO") Support: Contractor shall be responsible for supporting and executing the strategic and day-to-day aspects of the RMF and A&A life cycle processes in conjunction with and on behalf of the USAC CISO, USAC Information System Security Manager ("ISSM"), and the USAC IT Risk Champion (the USAC assigned risk leadership professional for IT). Contractor shall provide resources who are responsible for performing the following:

i. **Baseline A&A Support:**
    i. Generic A&A Support: In support of the ongoing maintenance and compliance of the A&A Program, Contractor shall:
        a. Provide A&A support for approximately 15 moderate baseline systems consisting of USAC Enterprise Common Controls ("ECC"), USAC-hosted systems, systems hosted on cloud-based platforms authorized by the Federal Risk and Authorization Management Program ("FedRAMP"), and systems hosted on non-FedRAMP-authorized cloud services.
        b. Develop and maintain a plan for USAC ISSM and CISO approval to maintain authorization or risk acceptance for all relevant systems, including achievement of Authorization to Operate ("ATO") for new or significantly changed systems, in accordance with appropriate Office of Management and Budget ("OMB"), NIST, and FISMA guidance/regulations as well as USAC policies. Develop and maintain the Information Security Program internal portal with A&A plan and associated ISSO responsibility matrix.
        c. Work with system owners and IT to

develop/update/maintain A&A materials in order to achieve ATO, Reauthorization, or continued authorization through Information Security Continuous Monitoring ("ISCM"), including support for third-party independent Security Controls Assessment ("SCA"), when initiated by USAC CISO.

d. Provide support to USAC's IT Security Compliance by:
    i. Preparing A&A packages, including a System Security Plan ("SSP") for each USAC system;
    ii. Strategically advising on the restructuring or reordering of system boundaries for compliance packages, as needed;
    iii. Preparing risk management recommendations; and
    iv. Tracking POA&Ms, both internally to OCISO and with system owners, as they are related to USAC's systems.
e. The A&A packages shall:
    i. Conform to NIST SP 800-18 (Guide for Developing Security Plans for Information Technology ("IT") Systems);
    ii. Clearly define the security requirements;
    iii. Describe the controls in place or plan to meet these requirements; and
    iv. Delineate the responsibilities and expected behavior of all individuals who access the system.
f. Provide RMF support in accordance with NIST SP 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems, latest version). This support shall include:
    i. Reviewing the system categorization of each USAC system with the appropriate stakeholders and determining if the current categorization is accurate in accordance with USAC and NIST guidelines;
    ii. Assisting system stakeholders in the process of updating or re-performing system categorizations in concurrence with the relevant requirements;
    iii. Assisting system owners, stakeholders, and USAC Privacy Officer ("PO") by facilitating meetings to perform Privacy Threshold Assessments ("PTA") in accordance with USAC and NIST guidance. Based upon the results of each system's PTA, work with the PO to recommend whether an Initial Privacy Assessment ("IPA") is required and assist, as directed by ISSM and CISO, the PO and system

stakeholders in performance of these efforts in accordance with guidance;

iv. Preparing a recommendation on the baseline of NIST controls based on the Security Categorization for the ISSM or CISO;
v. Preparing a narrative in the SSP that provides:
    1. A description of the application;
    2. Software inventory;
    3. Hardware inventory;
    4. Technical diagrams; and
    5. Other supporting information.
vi. Assisting in the selection of common controls. A common control is a control that can be applied in its entirety to one or more organizational information systems;
vii. Analyzing system documentation to determine if the SSP or equivalent document is accurate, updated, and:
    1. Includes a concise description of the information system;
    2. Confirms security category;
    3. Identifies potential threats; and
    4. Ensures security controls are adequately described.
viii. Documenting and uploading the controls into the USAC system of record for the control package in accordance to NIST SP 800-53 (latest revision). See Section 7. B. a. iv "IT Security Governance, Risk Management, and Compliance Tool Administration" for more details;
ix. Documenting potential or upcoming changes to the authorized or baselined system controls using USAC's Security Impact Analysis ("SIA") template to codify the potential or upcoming change and recommend to the ISSM and CISO whether the change necessitates re-assessment and reauthorization of the system;
x. Conducting internal risk assessments to ensure controls and countermeasures are identified to compensate for weaknesses to reduce risk to USAC operations, assets, individuals, or stakeholders;
xi. Reviewing and determining the extent that system security controls are implemented and operating in accordance with established security requirements;

xii. Serving as system liaison to the SCA, penetration tester, and for overall system for security purposes for both internal and external parties;
xiii. Compiling documentation and supporting materials required for each system assessment as directed by the SCA. The items to be compiled may depend on previous findings, audit results, and evidence of completion. Examples of items that could be included are, but are not limited to:
    1. SSP;
    2. Risk Assessment Report ("RAR");
    3. Contingency Plans and Test Results;
    4. System of Record Notice ("SORN");
    5. Federal Information Processing Standard ("FIPS") 199;
    6. Configuration Management Plan ("CMP");
    7. SIA;
    8. Cybersecurity and Privacy Incident Response Plan ("CPIRP");
    9. Disaster Recovery Plan ("DRP"); and
    10. NIST SP 800-47 Revision 1, Managing the Security of Information Exchanges, Information Exchange Security Management ("IESM") documents such as Memorandum of Understanding ("MOU") or Interconnection Security Agreement ("ISA").
xiv. Preparing risk determination statements outlining potential risk to USAC operations, assets, individuals, or stakeholders based on vulnerabilities inherent in USAC information technology systems. The risk determination statement shall include planned or completed corrective actions intended to reduce or eliminate vulnerabilities, and a recommendation in determining whether the risk to agency operations, assets, or individuals is within tolerable limits; and
xv. Validating updates to the SSPs based on the final determination of risk to USAC operations, assets, individuals, or stakeholders.

g. Prepare and submit to the USAC CISO the final A&A packages, including the ATO memo, to the system owner and RAR, in accordance with established procedures.
h. Advise application developers on security requirements

throughout system develop development life cycle ("SDLC").

i. Facilitate cadenced meetings with system owners and/or Business Relationship Managers ("BRM") to discuss security issues, initiatives, or changes.
j. Conduct A&A oversight of USAC's BPO vendor systems by reviewing A&A materials and monitoring security compliance status.
k. Analyze and develop plan for migration to latest revision of major relevant compliance publication/regulation (i.e. NIST Publications, FISMA, OMB Memoranda, Department of Homeland Security ("DHS") Directives/Binding Directives, etc.), as needed and directed by CISO, to include:
    i. Analyzing changes between revisions;
    ii. Assessing the impact on USAC's systems and processes; and
    iii. Developing an enterprise-level plan in coordination with USAC CISO which will document plans to implement the latest revision, including, but not limited to, updating SSPs, Policies, Procedures, and aiding in the implementation of new controls.
l. Provide quarterly reports on A&A activities to be used for an Executive Briefing to the Chief Information Officer ("CIO") and/or the USAC Enterprise Risk Management Council. These reports will include, at a minimum, the following headings:
    i. SCA Completed;
    ii. Penetration Tests Completed; and
    iii. Relevant POA&M Updates and Pending Activities;
    iv. Pending A&A Activities Needing Enterprise Attention.
m. Support the CISO in developing a provisioning process that reduces costs, improves productivity, enforces the appropriate security policies, and ensures compliance.

ii. ISCM Support and Internal Controls Testing: In addition to and in conjunction with contractor-provided A&A support referenced in Section 7. B. a. i. 1. "Generic A&A Support" for the purpose of providing support for the continued authorization and compliance of USAC systems, Contractor shall:
    a. Facilitate continuous monitoring of each USAC IT System, to include preparing A&A packages for new or reauthorized systems, in the USAC IT System portfolio by working with the CISO, ISSM, developers, and system owners.
    b. Update SSPs for each USAC application in the USAC's

system portfolio in accordance with the established plan (Section 7. B. i. f. v "IT Security Governance, Risk Management, and Compliance Tool Administration") working with the CISO, ISSM, developers, and system owners. The plans shall conform to NIST SP 800-18 (Guide for Developing Security Plans for Information Technology Systems).

c. Provide support for the USAC's implementation of the ISCM process. Such support shall include:
    i. Reviewing current USAC policies and procedures to identify compliance gaps with Federal requirements and determine which are applicable to the USAC's environment;
    ii. Integrating the identified gaps into the current USAC Cybersecurity Policy, as well as any other applicable procedural guidance issued by USAC;
    iii. Reviewing policies and procedures using a formalized process at a minimum annually and when directed;
    iv. Providing support to ISSM or CISO through the facilitation (e.g., leading, developing presentation materials, etc.) and attendance of weekly program, system, applicable security related, and general administrative meetings;
    v. Assisting system owners and stakeholders through the POA&M process documented in Section 7. F. "POA&M and Vulnerability Management Program Support";
    vi. Acting as liaisons between business functions/system representatives and the OCISO;
    vii. Assisting system representatives with security-related requests and inquiries. Examples of these requests and inquiries are, but are not limited to:
        1. Requests related to maintenance and/or modifications of existing systems;
        2. Initiatives for the implementation of new systems;
        3. Problem resolution;
    viii. Performing analysis of system CMPs to identify gaps in terms of compliance with federal requirements and ensure accuracy of the documentation as it relates to each system's current environment;
    ix. Assisting system owners in updating system CMPs through integration of the identified gaps into current

documentation;

x. Developing and implementing a formalized process to review system CMPs on a periodic basis, at least annually;
xi. Working with key organizational stakeholders to update the application/system contingency plans and the overall DRP based upon the identified gaps within the scope/constraints identified by USAC IT leadership;
xii. Reviewing the system categorization of each system with the appropriate stakeholders and determining if the current categorization is accurate in accordance with USAC and NIST guidelines;
xiii. Assisting system stakeholders in the process of updating or re-performing system categorizations in concurrence with the relevant requirements; and
xiv. Updating interconnection information for each system's documentation, i.e. ISAs, as necessary based upon the definition.

d. Ensure security controls remain effective over time by performing routine checks with appropriate stakeholders, i.e. IT Systems Operations, IT Security Operations, etc., and report gaps to the CISO. The activities/artifacts in-scope for review include, but are not limited to:
    i. Annual SCA assessments
    ii. Audit log reviews
    iii. Documentation updates
    iv. Vulnerability scanning and patching
    v. User account maintenance
    vi. Review of access lists
    vii. Third-party compliance monitoring
    viii. Relevant training
    ix. Incident response testing
    x. Configuration management
    xi. System element inventory
    xii. Key/combination/badge maintenance
    xiii. Risk designations
    xiv. Physical access monitoring
e. At the direction of the CISO, perform internal controls testing of a subset of systems or subsystems to assess the impact of minor changes to authorized systems, perform interim authorizations, and/or risk assessments. This testing can use NIST SP 800-53A (latest revision) as a guide for testing the implementation of controls or another approach

as agreed upon by the CISO.

f. At the direction of the CISO, conduct internal SCA activities, for minor systems, systems whose impact is determined to be internal-only or minimal, or systems whose annual Reauthorization or ISCM activities are too far in the future to support near-term requirements. Internal SCA activities, as directed, will extend to FedRAMP Software-as-a-Service ("SaaS") offerings from cloud service providers with limited customer responsibilities. This testing can use NIST SP 800-53A (latest revision) as a guide for testing the implementation of controls or another approach as agreed upon by the CISO.

C. Ongoing Security Authorization ("OSA") Program: As USAC matures in its authorization of systems, its implementation of ISCM, and its adoption of DevSecOps (development, security, and operations, automating the integration of security at every phase of the software development lifecycle), OCISO will drive the transition from legacy A&A practices to OSA. At the direction of the CISO, but no later than ("NLT") 18 months after award, contractor shall:

1. Develop a comprehensive plan to migrate systems to an OSA process that leverages the use of NIST SP 800-37 for Risk Management, NIST SP 800-53 for Control Guidance, and NIST SP 800-137 for Guidance on the Continuous Monitoring processes.
2. Ensure all system compliance, i.e. OMB, NIST, FISMA, remain in place as well as all interactions, collaboration, and communication with system owners and stakeholder continues as detailed in Section B.7. A. and B
3. Recommend innovative ways to administer the A&A activities necessary for OSA, i.e. automation ingrained into the testing of controls and reporting of results.
4. Ensure recent versions of NIST SP 800-53 control tests and any additional tests OCISO deem appropriate, e.g. penetration tests, be included for OSA.
5. Develop appropriate policies and procedures dictating the implementation and execution of OSA.
6. Develop and maintain an OSA master project schedule using NIST assessment methods and approved OSA procedures, including rules of engagement for each system moving to OSA.
7. Continue to review the SSPs annually and ensure that the Contingency Plans and CMPs are reviewed at least annually. Capture the results and when the plans were reviewed in the appropriate USAC repository.
8. Develop a process for addressing and mitigating identified system weaknesses in a timely manner in order to ensure systems continue to be eligible for OSA.

9. Create and submit to the CISO, a monthly OSA report that itemizes and describes the OSA scheduled assessment activities as well as the status of systems in the OSA.

D. Information Security Policies, Procedures, and Standards Management: Contractor shall be responsible for managing USAC's information security policies, procedures, and standards based on directives provided by FISMA, NIST, OMB, DHS, etc., by performing the following:

1. Update the current USAC A&A policies for each NIST SP 800-53 control) and USAC Information Security and Privacy Control Policy at least annually.
2. Identify gaps in USAC's Information Security and Privacy Control Policy NIST control family procedures. Provide quarterly reports on the identified gaps and recommended mitigation efforts. Assist with the development of the identified artifacts and/or mitigation efforts.
3. Assist with the implementation of these artifacts in USAC operations to include:
    a. Conduct research, analysis, and recommend changes to the USAC Information Security Policy at least annually.
    b. Maintain awareness of and report significant information-related policy issues affecting USAC via bi-weekly status meetings.
4. Review and provided recommend changes to the USAC Information Security Policy at least annually.
5. Update Policies and Procedures content on the internal Information Security Program site, as needed.
6. Develop, update, and maintain an ISSO SOP and management directive that will inform and guide the activities and responsibilities of the ISSOs in support of OCISO.

E. IT Security Governance, Risk Management, and Compliance ("GRC") Tool Administration: Contractor shall be responsible for the administration and maintenance of USAC's system of record for control packages and SSPs, the USAC IT Security GRC Tool. Currently, USAC utilizes Telos Xacta 360 as its IT Security GRC Tool, but this system could change in the future based on contractor's recommendation and/or at the direction of the CISO. The contractor shall:

1. Manage standard operations and maintenance of the GRC Tool to assist with the A&A process. These activities include capturing, organizing, and maintaining all draft and final security artifacts in the GRC repository and implementing an approved system categorization to support the Enterprise architecture standards developed by USAC.
2. Support the independent third-party assessors that will use the GRC tool during the assessment for artifact collection and SRTM preparation.
3. Support the ISSM and CISO in the registration, completion, and

maintenance of the GRC Tool projects/packages for the information systems.

4. Assist OCISO and IT Systems Operations in the daily secure operation of the GRC Tool.
5. Ensure audit logs are reviewed and conduct regular audits to ensure security and accountability on an as needed basis. Also, work with the IT Security Operations to integration audit logging into the USAC Security Information and Event Management ("SIEM") tool, if possible.
6. Ensure the ISSM approves User access privileges and ensure User access is validated periodically by the ISSM, in coordination with the Identity and Access Management ("IAM") team, to ensure the User requires continued access to the system and correct privileges are assigned. These reviews must take place at least quarterly.
7. Ensure all departing users have their access privileges terminated immediately. Termination of access also applies to users whose job functions have changed and they no longer require access to the level to which they were previously granted.
8. Contractor shall ensure separation of duties is enforced through technical mechanisms, as needed.
9. Ensure unused or inactive accounts are reviewed and deactivated monthly in collaboration with the IAM team. Consult internal USAC policies and procedures for the definition of an inactive account.

F. POA&M and Vulnerability Management Program Support: Contractor shall be responsible for managing the strategic and day-to-day aspects of the POA&M and vulnerability management at USAC in conjunction with or on behalf of the CISO and the USAC Security Governance Lead (the individual assigned to monitor and guide conformance to security guidance and directives). Contractor shall perform the following activities:

i. POA&M Management Program:

1. Develop and maintain a plan which will codify the purpose and responsibilities of the POA&M Management Program ("POA&M Management Program Plan"). Provide updates at least annually.
2. Develop and maintain the USAC POA&M Management Procedure with updates provided at least annually. Manage the POA&M process, and seek to improve USAC's formal process to approve POA&Ms, which involves active participation from system stakeholders.
3. Perform continual analysis of POA&M management to identify gaps and opportunities for improvement, providing potential improvement recommendations at least quarterly.
4. Schedule and facilitate, as required, meetings with ISSOs, system owners, and key stakeholders to track and assist in the remediation

of POA&Ms.

5. Manage and coordinate the creation of new POA&Ms as new findings arise from designated POA&M sources (including, but not limited to A&A assessments, audits, incidents, penetration test findings, etc.).
6. Manage and update POA&Ms in accordance established plan via regular interactions with the ISSOs, system owners, and other relevant stakeholders.
7. Manage and coordinate the collection of evidence and closure of POA&Ms with ISSOs, system owners, and other relevant stakeholders. Use the USAC-designated software for tracking all POA&Ms and associated details. Currently, USAC utilizes JIRA software to manage POA&M data, but this system could change in the future based on contractor's recommendation and/or at the direction of the CISO.
8. Document and remediate POA&Ms working with OCISO, developers, system owners, and other key stakeholders.
9. Ensure POA&M due dates and milestone dates within the system are monitored closely and updated as necessary to achieve goals and produce accurate reporting of POA&M status.
10. Advise system stakeholders on upcoming due dates relating to milestones and overall completion of POA&Ms.
11. Assist in the implementation and formalization of all related risk acceptance documentation.
12. Provide trending and metrics reports on POA&Ms as part of the Information Security Program Metrics deliverable on at least a bi-weekly basis. These reports will include, at a minimum:
    a. POA&M trending graphs, including POA&Ms by severity, USAC system, and BPO;
    b. Delayed POA&Ms, including POA&Ms expected to be delayed in the next two weeks;
    c. Open POA&Ms;
    d. Closed POA&Ms; and
    e. Risk Accepted POA&Ms.
13. Provide bi-weekly trending and metrics reports on POA&Ms to be used for an Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team. These reports will include, at a minimum:
    a. POA&M trending graphs, including POA&Ms by severity, USAC system, and BPO;
    b. Delayed POA&Ms, with a call-out to key POA&M with enterprise implications;
    c. Open POA&Ms, with a call-out to key POA&M with enterprise implications; and

d. Closed POA&Ms.

14. Distribute the approved monthly reports to the CISO and/or designee.

ii. Vulnerability Management Program:

1. Develop and maintain a plan which will codify the purpose and responsibilities of the Vulnerability Management Program ("Vulnerability Management Program Plan"). Provide updates at least annually.
2. Develop and maintain the USAC Vulnerability Management Procedure with updates provided at least annually. The procedure will document a process, to include roles and responsibilities, for:
    a. Developing and proposing patch remediation and vulnerability assessment timelines, frequencies, and schedules;
    b. Verifying successful remediation before weakness closure; and
    c. Defining a programmatic approach to remediating vulnerabilities prior to meeting defined POA&M tracking thresholds, if applicable.
3. Perform continual analysis of the USAC's vulnerability management to identify gaps and opportunities for improvement, providing potential improvement recommendations at least quarterly.
4. Manage and coordinate tracking and closure of system vulnerabilities (including code-based vulnerabilities) with ISSOs, developers, system owners, and other stakeholders. Currently, USAC utilizes Tenable as its vulnerability scanning tool, but this system could change in the future based on contractor's recommendation and/or at the direction of the CISO. Additionally, the contractor is expected to provide a recommendation for the best tool to track vulnerabilities.
    a. Contractor will be required to perform analysis on weekly security scans to facilitate discussions with system teams, ISSOs and other stakeholders.
    b. Contractor will work with security operations team to track and manage any vulnerabilities that require risk acceptance in the Tenable tool.
5. Work with Security Operations team to generate and provide trending and metrics reports on vulnerabilities as part of the Information Security Program Metrics deliverable on at least a bi-weekly basis. These reports will include, at a minimum:
    a. Vulnerability trending graphs overall and by system;
    b. Vulnerability age tracking overall and by system; and
    c. Vulnerability severity tracking overall and by system.

6. Provide weekly trending and metrics reports on vulnerabilities to be used for an Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team. These reports will include, at a minimum:
    a. Vulnerability trending graphs overall and by system;
    b. Vulnerability age tracking overall and by system, with a call-out to key vulnerabilities with enterprise implications; and
    c. Vulnerability severity tracking overall and by system, with a call-out to key vulnerabilities with enterprise implications.
7. Schedule and facilitate, as required, meetings with ISSOs, system owners, and key stakeholders to track and assist in the remediation of vulnerabilities.
8. Provide support for Cyber Hygiene (a set of proactive practices for mitigating attack vectors to maintain the security of users, devices, networks and data) by developing and executing procedures for capturing and tracking through to remediation all vulnerabilities reported by federal sources, i.e. DHS, or as required by federal directives, such as DHS Binding Operational Directive 22-01, using the same methodologies. Generate specific reports for vulnerabilities identified by federal sources on at least a bi-weekly basis.

G. IT Risk Management Program: Contractor shall be responsible for establishing and managing the strategic and day-to-day aspects of an information technology risk management program as defined in OMB Circular A-123, OMB Circular A-130, and other relevant federal guidance and memoranda ("IT Risk Management Program") in conjunction with or on behalf of the USAC IT Risk Champion. Contractor shall perform the following activities:

i. Assist in the development of an IT Risk Management Programby:
    1. Developing and maintaining an IT Risk Management Program Charter which will codify the purpose and responsibilities of the IT Risk Management Program. Provide updates at least annually;
    2. Developing and maintaining the IT Risk Management Program Plan, with updates provided at least annually, to define, at least, the structure, cadence, and organization of the IT Risk Management Program, and an associated implementation plan, which will, at least, detail how to communicate, train, and monitor the IT Risk Management Program on an enterprise level;
    3. Developing a process and/or communication plan to capture and report risk-related issues to IT leadership for final risk governance review;
    4. Providing quarterly trending and metrics reports on IT risks to be used for an Executive Briefing to the CIO and/or the USAC Enterprise Risk Management Council; and
    5. Performing continual analysis of the IT Risk Management Program

to identify gaps and opportunities for improvement, providing potential improvement recommendations at least quarterly.

ii. Manage and coordinate tracking and closure of IT risks in conjunction with, a collaborative risk program operated at the USAC enterprise level ("Enterprise Risk Management"), by:
    1. Recommending an automated mechanism for capturing and tracking IT risks;
    2. Scheduling and facilitating, as required, meetings with ISSOs, system owners, and key stakeholders to track and assist in the identification and governance of IT risks;
    3. Defining the overall IT risk appetite and risk governance methodology;
    4. Developing risk tracking metrics, inclusive of, at least, severity, program, and financial implications; and
    5. Identifying critical risk thresholds with respect to information system security.

H. Supply Chain Risk Management ("SCRM") Program: The SCRM Program will provide awareness on supply chain risk from threat nations and other attack vectors in accordance with the National Defense Authorization Act ("NDAA") for Fiscal Year ("FY") 2019, Executive Order ("EO") 14028 (Improving the Nation's Cybersecurity), and other relevant Orders from the FCC. Contractor shall be responsible establishing and managing the strategic and day-to-day aspects of the SCRM Program in conjunction with or on behalf of the CISO. The contractor shall perform the following activities:

i. Develop and maintain an SCRM program charter which will codify the purpose and responsibilities of the SCRM Program. Provide updates at least annually.
ii. Develop and maintain the SCRM program plan, with updates provided at least annually, to define, at least, the structure, cadence, and organization of the SCRM Program, and an associated implementation plan, which will, at least, detail how to communicate, train, and monitor the SCRM Program on an enterprise level.
iii. Perform continual analysis of the SCRM Program to identify gaps and opportunities for improvement, providing potential improvement recommendations at least quarterly. Sources for gap analysis include, but are not limited to, updated OMB, NIST, DHS, and congressional guidance.
iv. Operate and enhance a SCRM Program with vendor risk intelligence and continuous monitoring with integrations with, at least, IT Architecture and Standards, USAC Procurement Team, and USAC Office of General Counsel ("OGC") in coordination with CISO.
v. Collaborate with the ISSOs and other relevant stakeholder, i.e. Procurement Team and OGC, to define appropriate policies and procedures for executing an enterprise SCRM.
vi. Document risk mitigation recommendations and communicate to stakeholders.

vii. Store all documentation and resources in the CISO-approved document repository.
viii. Develop Objectives and Key Results ("OKR") to demonstrate program success including, but not limited to:
    1. Quantity of SCRM support requests;
    2. Risk threshold determinations;
    3. Quantity of customers and impact to enterprise; and
    4. Productivity-oriented metrics.
ix. Provide quarterly trending and metrics reports on OKRs to be used for an Executive Briefing to the CIO and/or the USAC Enterprise Risk Management Council.

I. Transition In or Out Services: As tasked, Contractor shall facilitate the transition of contracted activities and services to USAC personnel or to a follow-on contractor at the beginning or at the end of the contract period of performance. Representative activities under this task area may include:

a. Provide USAC with current versions of all system and user documentation;
b. Provide USAC all licensing and renewal information, asset management records, software documentation, and training materials;
c. Provide USAC with a current inventory of all USAC-owned assets used by the contractor along with full support in the reconciliation of this inventory;
d. Provide USAC with current versions of all operational procedures, standard operating procedures, guidelines, performance reports, specifications for hardware and software, in-flight activities, and other pertinent information needed to continue the services being performed by Contractor; and
e. Provide "shadowing" and other knowledge transfer meetings and opportunities to facilitate the transfer of information, processes, and data needed to continue the services being performed by Contractor.

J. Key Personnel: Contractor shall provide consultant staffing for one (1) or more of the following labor categories:

a. Program Manager (CISSP or equivalent): Contractor shall designate one (1) key personnel with at least 10 years of relevant cybersecurity program management experience to oversee the project, act as the day-to-day contact for USAC, and serve as senior technical advisor to CISO and OCISO staff and it relates to the scope of this contract.

b. ISSO Lead (CISSP, CIPT or equivalent): Contractor shall designate key personnel to lead the ISSO capability by planning for and carrying out A&A support activities as well as developing and implementing information security standards and procedures.

c. POA&M Management Lead (CISSP or equivalent/appropriate): Contractor shall designate key personnel to lead the POA&M Management Program by planning for and carrying out POA&M Management activities.

d. Vulnerability Management Lead (CISSP or equivalent/appropriate): Contractor shall designate key personnel to lead the Vulnerability Management Program by planning for and carrying out Vulnerability Management activities.

e. **Risk Management Lead (PMP, PMI-RMP, CRISC, or equivalent):** Contractor shall designate key personnel to lead the IT Risk Management Program by planning for, implementing, and executing the IT Risk Management Program.
f. **Supply Chain Risk Management Lead (PMP, PMI-RMP, CRISC, or equivalent/appropriate):** Contractor shall designate key personnel to lead the IT Supply Chain Risk Management Program by planning for, implementing, and executing the IT Supply Chain Risk Management Program.

K. Applicable Documents: The work to be performed under this contract will assist USAC in better meeting legislative mandates and associated implementation guidance from OMB, NIST, DHS, FCC, and other Federal agencies. Contractor must comply with, but not limited to, the following Statutes, and Acts:

a. Computer Security Act of 1987, PL 100-235
b. Federal Information Security Modernization Act of 2014 (FISMA)
c. Federal Cybersecurity Workforce Assessment Act of 2015
d. OMB Memorandum M-14-03: Enhancing the Security of Federal Information and Information Systems.
e. OMB Circular A-130 and Appendix III, Security of Federal Automated Information Resources
f. OMB Circular A-123, Management's Responsibility for Internal Control
g. Presidential Decision Directives
h. Executive Orders (such as 14028)
i. NIST Cybersecurity Framework
j. USAC, current policies for Information Systems Security and Privacy
k. E-Government Act of 2002
l. Clinger-Cohen Act of 1996
m. Computer Fraud and Abuse Act of 1986
n. NIST Special Publications – 800 Series
o. NIST Federal Information Processing Standards
p. The Privacy Act of 1974
q. Section 508 of the Rehabilitation Act of 1973

L. Deliverables

Contractor shall provide the following deliverables in accordance with terms set forth below and in Section C of this RFP.

#	Frequency	Deliverable	Description
01	Ongoing	A&A Materials for all USAC systems	All materials needed for the authorization and/or ISCM of all USAC IT Systems including, but not limited to: • SSPs • RARs • POA&Ms • ATO Memos • Contingency Plan and Test • FIPS 199 • CMP • ISAs/MOUs • SIAs (as needed)
02	Monthly	System Assessment, Authorization and Continuous Monitoring Project Plans	Project plans for A&A and ISCM activities throughout the year for each USAC IT System presented to the CISO for monthly review, including progress on all relevant A&A and ISCM materials
03	Bi-weekly	A&A Dashboard (to be used for Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team)	Roll-up of all A&A Activities Planned, Ongoing, and Completed per USAC IT System in each calendar year including, but not limited to: • Key A&A Dates/Milestones • System Owner • Latest A&A Activity/Update • Latest System Activity/Update
04	Quarterly	Quarterly A&A Reports on Program Compliance activities	Report of all A&A Activities Planned, Ongoing, and Completed per USACIT Ssystem including, but not limited to: • Pending A&A Activities Needing Enterprise Attention • SCA Activities • Penetration Testing • POA&M Metrics • Vulnerability Metrics

#	Frequency	Deliverable	Description
05	As Needed	Security Impact Analysis	Document potential or upcoming changes to the authorized or baselined system controls for the purpose of codifying the potential or upcoming change and recommend to the ISSM and CISO whether the change necessitates re-assessment and reauthorization of the USAC IT System.
06	As Needed	Internal Risk Assessment	Identify and formally document controls and countermeasures which are identified to compensate for weaknesses to reduce risk to USAC operations, assets, individuals, or stakeholders.
07	As Needed	Risk Determination Statements	Identifying and formally outlining potential risk to USAC operations, assets, individuals, or stakeholders based on vulnerabilities inherent in USAC IT Systems.
08	Bi-weekly	System Owner/System Team/BRM Meeting Output	Meeting minutes from meetings with system owner/system team/BRMs after regular meetings on the topic of status and planned activities/changes to the respective systems; to be provided NLT two (2) business days after the meeting takes place.
09	Annual (initial review in base year and annual thereafter)	BPO A&A Material Review	Review of BPO-submitted A&A materials completeness, accuracy, and effectiveness with recommendations to be provided to the CISO.
10	Monthly	BPO POA&M Review	Review of BPO-submitted POA&Ms for completeness, accuracy, and effectiveness with recommendations to be provided to the CISO.
11	As Needed	Action Plan for Implementing Major Relevant Compliance Publication/Regulation	Analyze and develop plan for migration to latest revision of major relevant compliance publication/regulation (i.e. NIST Publications, FISMA, OMB Memoranda, DHS Directives/Binding Directives, etc.), as needed and directed by CISO.

#	Frequency	Deliverable	Description
12	As Needed (NLT two business days after meeting)	Provide Detailed Meeting Minutes	Document and provide meeting minutes from meetings with assessors/auditors, BRMs, system owners, and other regularly assigned meetings; to be provided NLT two (2) business days after the meeting takes place; minutes to include, but are not limited to, meeting attendees, action items, and general notes of conversations/discussion topics.
13	One-time (with annual update)	Process for Facilitating System Authorization and ISCM Activities	Document and submit for approval formal process for carrying out activities enumerated in Section 7. B. i. "ISCM Support and Internal Controls Testing"
14	As Needed	Internal Controls Testing Results	Perform internal controls testing of a subset of systems or subsystems to assess the impact of minor changes to authorized systems, perform interim authorizations, and/or risk assessments.
15	As Needed	Internal SCA Results	Conduct internal SCA activities, for minor systems, systems whose impact is determined to be internal-only or minimal, or systems whose annual Reauthorization or ISCM activities are too far in the future to support near-term requirements
16	One-time NLT 18 months after contract award (with subsequent annual update)	OSA Migration Plan	Develop a comprehensive plan to migrate systems to an OSA process that leverages the use of NIST SP 800-37 for Risk Management, NIST SP 800-53 for Control Guidance, and NIST SP 800-137 for Guidance on the Continuous Monitoring processes (includes all sub-activities in Section B. 7. C. "Ongoing Security Authorization ("OSA") Program" as well as recommendations for updating existing A&A-related deliverables)
17	One-time (with monthly updates thereafter)	OSA Master Project Schedule (after delivery and acceptance of #16)	A comprehensive schedule reflecting milestones and deadlines using NIST assessment methods and approved OSA procedures.

#	Frequency	Deliverable	Description
18	One-time (with annual update)	OSA Process Plan (after delivery and acceptance of #16)	A process for addressing and mitigating identified system weaknesses to ensure systems continue to be eligible for the OSA program.
19	Monthly	OSA Status Report (after delivery and acceptance of #16)	Create and submit monthly OSA report that itemizes and describes the OSA scheduled assessment activities as well as the status of systems in the OSA.
20	One-time (with annual update)	Inventory of all USAC IT Security Policies, Procedures and Standards	Provide an inventory of all existing USAC IT Security Policies, Procedures and Standards.
21	Quarterly	Information Security and Privacy Control Policy Gap Analysis	Provide quarterly reports on the identified gaps and recommended mitigation efforts. Assist with the development of the identified artifacts and/or mitigation efforts.
22	Annual	Updates of all A&A policies	Provides updates to the USAC A&A policies for each NIST SP 800-53 control and USAC Information Security and Privacy Control Policy.
23	As Needed	Updates on internal Information Security Program site	Update Policies, Procedures, and Standards content on the internal Information Security Program site.
24	One-time (with annual update)	ISSO SOP and Management Directive	Develop, update, and maintain an ISSO SOP and management directive that will inform and guide the activities and responsibilities of the ISSOs in support of OCISO.
25	Ongoing	GRC Information Management	Capture, organize, and maintain all draft and final A&A security artifacts in the USAC IT Security GRC Tool and other repositories as directed, and maintain system categorization/documentation for support of A&A activities, SCA, FISMA audit, etc.

#	Frequency	Deliverable	Description
26	Ongoing	GRC Tool Administration	Ensure the security and effective use of the IT Security GRC Tool, including the implementation of system patches, integration with USAC's SIEM, user access reviews, separation of duties, etc.
27	One-time (with annual update)	POA&M Management Program Plan	Maintain and update the USAC POA&M Management Plan.
28	One-time (with annual update)	POA&M Management Procedure	Document the tactical responsibilities of the POA&M Management Program, including the collection, management, and reporting of POA&Ms.
29	Ongoing	POA&M Documentation Management	Manage and maintain all POA&Ms in the USAC-defined USAC IT System.
30	Bi-weekly	POA&M Metrics (to be used for Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team)	Provide POA&M metrics which includes, but not limited to: • POA&M trending graphs • Delayed POA&Ms • Open POA&Ms • Closed POA&Ms • Risk Accepted POA&Ms
31	One-time (with annual update)	Vulnerability Management Program Plan	Maintain and update the USAC Vulnerability Management Plan.
32	Monthly	Business Relationship Managers (BRM) Dashboard	Provide updated program POA&M and vulnerability status and risk exposure for each program area.

#	Frequency	Deliverable	Description
33	One-time (with annual update)	Vulnerability Management Procedure	Maintain and update the USAC Vulnerability Management Plan. The plan documents a process for: • Developing and proposing patch remediation and vulnerability assessment timelines, frequencies, and schedules. • Verifying successful remediation before weakness closure. • Defining a programmatic approach to remediating vulnerabilities prior to meeting defined POA&M tracking thresholds.
34	Weekly	Vulnerability Metrics (to be used for Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team)	Vulnerability metrics which includes (at a minimum) trending graphs communicating the characteristics and severity of overall vulnerabilities of USAC IT Systems.
35	Ongoing	Vulnerability Documentation Management	Identify and track system vulnerabilities with system owners using a tool identified by USAC.
36	One-time (with annual update)	Cyber Risk Management Charter and Program Plan	Development of a Risk Management Charter and Program Plan .
37	Monthly	Metrics for tracking Cyber Risk Management (to be used for Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team)	Monthly metrics to track cyber risk management, to include, but not limited to, risk trending graphs, overdue risks, current risks, risks by severity and business groups (to include IT risks).
38	One-time	Risk Management Implementation Plan	A plan outlining how to implement the risk management charter/plan into the organization.
39	One-time (with annual update)	Risk Management Communications Plan	A plan/process to capture and communicate risk related issues within information security as well as IT department.

#	Frequency	Deliverable	Description
40	One-time (with annual update)	SCRM Program Charter	Maintain and update the SCRM Program Charter which will codify the purpose and responsibilities of the SCRM Program.
41	One-time (with annual update)	SCRM Program Plan	SCRM Program Plan to define, at least, the structure, cadence, and organization of the SCRM Program.
42	One-time (with annual update)	SCRM Program Policies and Procedures	Define and documented appropriate policies and procedures for executing an enterprise SCRM.
43	One-time	SCRM Program Implementation Plan	Details how to communicate, train, and monitor the SCRM program on an enterprise level.
44	Ongoing	SCRM Program Operations	Operate and enhance a SCRM Program with vendor risk intelligence and continuous monitoring with USAC team integrations; document risk mitigation recommendations and communicate to stakeholders; store all documentation and resources in the CISO-approved document repository.
45	One-time (with quarterly reporting)	Develop OKR and Associated Trending and Metrics Reports on OKRs (to be used for Executive Briefing to the CIO, the USAC Enterprise Risk Management Council, and/or the FCC IT Security Team)	Develop objectives to demonstrate program success including but not limited to: quantity of SCRM requests; risk threshold determinations; quantity of customers and impact to enterprise; productivity-oriented metrics.
46	One-time	Transition In Plan (within five (5) business days of contract award)	Develop a 60-day plan for onboarding all resources and providing support for USAC teams and deliverables as described in Section B. 7. I. “Transition In or Out Services”.
47	One-time	Transition Out Plan (NLT 60 days before end of contract period of performance)	Develop a 60-day plan for onboarding resources and providing support for USAC teams for the knowledge transfer of all deliverables and responsibilities as described in Section B. 7. I. “Transition In or Out Services”.

#	Frequency	Deliverable	Description
48	One-time (with monthly update)	Deliverable Schedule	Develop a proposed comprehensive deliverable schedule incorporating all deliverables contained in this section (Section B. 7. L. "Deliverables") and when the Contractor proposes these to be delivered; proposed deliverable schedule to be presented for approval by USAC and reviewed at least monthly. *Note: all deliverables need to be accompanied by a Deliverable Acceptance Form (DAF) in order to be formally accepted by USAC*
49	Weekly	Weekly Status Report	Provide an informal weekly consolidated update of all activities performed during the preceding week as well as planned activities for the subsequent week.
50	Monthly	Monthly Status Report	Provide a formal report of major/significant activities and accomplishments performed during the preceding month as well as planned major/significant activities for the subsequent month to be communicated to USAC leadership.

8. MEETINGS

1. Project Kick-Off Meeting.
   a. Within five (5) business days of the Contract effective 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 and transition-in plan. Contractor shall discuss the overall understanding of the project and review the background information and materials provided by USAC.

   b. 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.

   c. Contractor shall present the project plan to USAC for discussion and approval. The project plan should detail the agile process for reporting and remediating critical and high findings prior to issuing the final deliverables. A concerted effort shall be made to gain a thorough understanding of USAC's expectations. However, nothing discussed in this, or in any subsequent meetings or discussions between USAC and Contractor shall be construed as adding to, deleting, or modifying any Contract requirements, including deliverable specifications and due dates. All Contract

modifications and amendments must be approved in writing by an authorized USAC Procurement representative.

2. Weekly Status Meetings.
   a. Key personnel must schedule and participate in weekly status meetings and travel to USAC's office in accordance with the requirements of the Contract.

   b. Contractor shall prepare a status report and submit it to USAC once per week. The report must include the current status for each of the project work streams including percentage of completion, achievements and any risks/issues relating to Contract performance or payment. The report must include an expected completion date and the circumstances surrounding any possible delays. The report shall be submitted one (1) business day before each regularly scheduled status meeting and no later than Friday noon (12:00 PM ET) during weeks in which the meeting is scheduled for Monday or when no status meeting is scheduled. The Twice Weekly Status Report shall be used as the basis of the status meeting discussion.

3. Milestone Status Meetings.
   a. Key personnel must be prepared to present each deliverable either in-person or via webcast meeting, as directed by USAC. For revision rounds, the Contractor's key personnel should be prepared to walk through any editing round questions via phone.

   b. Key personnel must be prepared to provide interim deliverable updates, as requested by USAC.

4. Accessibility. Key personnel must be accessible via telephone or email during USAC's normal business hours, Monday through Friday (9:00 AM - 6:00 PM ET).

SECTION C:

USAC Terms and Conditions

1. DEFINITIONS

A. "Added Service" means a service that Contractor may perform for USAC that is not specified in the Scope of Work part of the Contract.

B. "Cloud Protocols" means a comprehensive information security program governing standard technical configurations, platforms, or sets of procedures used in connection with the Services operated in cloud infrastructure environments.

C. "Code" means the United States Bankruptcy Code.

D. "Confidential Information" is defined in Section 16 of these USAC Terms and Conditions.

E. "Contract" means these USAC Terms and Conditions, and any documents attached to these USAC Terms and Conditions that constitutes the entire agreement between the parties with respect to the subject matter hereof.

F. "Contract Term" means the Initial Term of these USAC Terms and Conditions and any executed Optional Renewal Terms.

G. "Contractor" means the Offeror (as defined elsewhere in the Contract) whose proposal was selected for award of the Contract.

H. "Contractor Owned/Controlled IT" means any devices, equipment, systems, or environments owned or controlled by Contractor.

I. "Contractor's IT System" means Contractor's electronic computing and/or communications systems (including but not limited to various internet, intranet, extranet, email and voice mail).

J. "Contractor Personnel" means Contractor's employees, subcontractors, consultants, and agents used to provide Services and/or create Deliverables under this Contract, including, but not limited to, Key Personnel. "Contractor Personnel" also includes the entity that employs Contractor's employees, subcontractors, consultants, and agents in all cases except where the context clearly references only individuals.

K. "COTS" means commercial off-the-shelf Software.

L. "Courts" means the district and, if applicable, federal courts located in the District of Columbia.

M. "CSP" means the USAC Coupa Supplier Portal, which is a method of paying USAC invoices.

N. "Data" means information, regardless of the form or media.

O. "Data at Rest" is defined in Section 18.H of these USAC Terms and Conditions.

P. "Data Breach" means" the loss of control, compromise, unauthorized disclosure, unauthorized movement, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses USAC's sensitive information (including PII, Data, Confidential Information, USAC Information) and/or USAC IT Systems or (2) an authorized user accesses or potentially accesses USAC's sensitive information (including PII, Data, Confidential Information, USAC Information) and/or USAC IT Systems for any unauthorized purpose. Types of Data Breaches include, but are not limited to, Data Loss, Data Theft, and Exfiltration.

Q. "Data in Transit" is defined in Section 18.H of these USAC Terms and Conditions.

R. "Data Loss" means the result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party.

S. "Data Security Laws" is defined in Section 18.A of these USAC Terms and Conditions.

T. "Data Security Liaison" is defined in Section 18.C of these USAC Terms and Conditions.

U. "Data Theft" means the deliberate or intentional act of stealing of information.

V. "Deliverables" means the goods, items, products, and materials that are to be prepared by Contractor and delivered to USAC as described in the Contract.

W. "Derivative Works" means any and all modifications or enhancements to, or any new work based on, in whole or in part, any USAC Information, Confidential Information, Data, Software, or Deliverable regardless of whether such modifications,

enhancements or new work is defined as a "derivative work" in the Copyright Act of 1976.

X. "Discloser" means a party to this Contract that discloses Confidential Information to the Recipient.

Y. "Exfiltration" means the unauthorized transfer of information from USAC IT Systems.

Z. "FCC" means the Federal Communications Commission, including, but not limited to, the Office of the Managing Director, the Office of Economics and Analytics, the Wireless Telecommunications Bureau, the Enforcement Bureau, the Wireline Competition Bureau, and the Public Safety and Homeland Security Bureau.

AA. "FedRAMP-Authorized Designation" means a cloud product or service that satisfies the security assessment, authorization, and continuous monitoring requirements of the Federal Risk and Authorization Management Program (or "FedRAMP").

BB. "FIPS" means Federal Information Processing Standard.

CC. "FISMA" means the Federal Information Security Management Act, 44 U.S.C. §3541, *et seq*., as amended by the Federal Information Security Modernization Act of 2014, and their implementing and successor regulations.

DD. "Initial Term" means the original duration of these USAC Terms and Conditions as described in Section 2 of these USAC Terms and Conditions.

EE. "IaaS" means Infrastructure as a Solution.

FF. "Key Personnel" means the full-time employees of Contractor that are in the positions identified elsewhere in the Contract as those that are required to perform the Services.

GG. "Malicious Code" or "Malware" means any software, firmware, program, routine, protocol, script, code, command, logic, or other feature that performs an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system and that is: (a) is designed to (i) disrupt, disable, deactivate, interfere with, or otherwise compromise USAC IT Systems, or (ii) access, modify, disclose, transmit, or delete PII, Data, Confidential Information, or USAC Information; or (b) either inadvertently or upon the occurrence of a certain event, compromises the confidentiality, integrity, privacy, security, or availability of PII, Data, Confidential Information, USAC Information, or USAC IT Systems. Examples

of Malicious Code include, but are not limited to, viruses, worms, bugs, ransomware, spyware, bots, backdoors, devices, and Trojan Horses.

HH. "Malicious Cyber Activity" means any activity, other than those activities authorized by or in accordance with any U.S. federal or state law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

II. "Multifactor Authentication" means a type of authentication using two or more factors to achieve verification of the identity of a user, process or device as a prerequisite to allowing access to an information system. A user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

JJ. "NARA" means the National Archives and Records Administration.

KK. "NIST" means the National Institute of Standards and Technology.

LL. "OMB" means the Office of Management and Budget.

MM. "Optional Renewal Term" means an additional one year period that can extend the duration of these USAC Terms and Conditions at USAC's sole discretion as described in Section 2 of these USAC Terms and Conditions.

NN. "PaaS" means Platform as a Service.

OO. "PII" means Personally Identifiable Information, which is 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.

PP. "Procurement Regulations" mean the following 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.

QQ. "Recipient" means a party to this Contract that receives Confidential Information from a Discloser.

RR. "SaaS" means Software as a Service.

SS. "SAM" means the System for Award Management or suspension or debarment status of proposed subcontractors that can be found at https://www.sam.gov.

TT. "SAN" means the Supplier Actionable Notification, which is a method of paying USAC invoices.

UU. "Security Incident" means any event or occurrence that actually or potentially compromises or jeopardizes the confidentiality, integrity, privacy, security, or availability of PII, Data, Confidential Information, USAC Information, or USAC IT Systems regardless of whether such event or occurrence: (a) poses a material or imminent threat to such PII, Data, Confidential Information, USAC Information, or USAC IT Systems, or (b) results in a Data Breach. Without limiting the foregoing, any attempt to compromise or jeopardize the confidentiality, integrity, privacy, security, or availability of PII, Data, Confidential Information, USAC Information, or USAC IT Systems or USAC's access to or use thereof, shall be considered a Security Incident.

VV. "Services" means the services, tasks, functions and responsibilities described in the Contract.

WW. "Software" means any application programming interface, content management system or any other computer programs, protocols, and commands that allow or cause a computer to perform a specific operation or series of operations, together with all Derivative Works thereof.

XX. "Solicitation" means the request for Services described in the Contract.

YY. "Sub-Recipient" means a partner, joint venturer, director, employee, agent and subcontractors of a Recipient to whom a Recipient must disclose Confidential Information.

ZZ. "USAC" means Universal Services Administrative Company.

AAA. "USAC Information" means any Data, materials, or communications in any form or format, whether tangible or intangible, spoken or written (regardless of media) 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 Derivative

Works thereof. All USAC Information is Confidential Information and subject to all requirements in Section 16 of these USAC Terms and Conditions.

BBB. "USAC IT System(s)" means USAC's electronic computing and/or communications systems (including but not limited to various internet, intranet, extranet, email and voice mail).

CCC. "USAC Terms and Conditions" means this document that provides the legal terms that govern this Contract.

DDD. "USF" means the Universal Service Fund.

2. TERM

The Initial Term is the period of time of one year after the Effective Date (as defined in the Contract) of the Contract. After the conclusion of the Initial Term, USAC will have the right to extend the Contract Term by exercising up to three (3) one-year Optional Renewal Terms. USAC may exercise an Optional Renewal Term by written notice to Contractor within ten (10) days prior to expiration of the then current Initial Term or Optional Renewal Term.

3. ACCEPTANCE / REJECTION

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.

USAC will only accept Services or Deliverables that meet the acceptance criteria described in a statement of work or scope of work to the Contract. If the Service or Deliverable is Software or hardware intended for USAC IT Systems, USAC will require acceptance testing during an acceptance period that will be described in a statement of work or scope of work to the Contract.

USAC will reject any Service or Deliverable that does not conform to the acceptance criteria described in a Statement of Work or Scope of Work to the Contract. 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 does not cure the defects within thirty (30) calendar days or if curing the defects is not possible, USAC may terminate for cause under Section 12 of these USAC Terms and Conditions, 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.

4. ENTIRE CONTRACT / BINDING EFFECT

The Contract supersedes and replaces all prior or contemporaneous representations, dealings, understandings or agreements, written or oral, regarding such subject matter. In the event of any conflict between these USAC Terms and Conditions and any other document made part of the Contract, the USAC Terms and Conditions shall supersede. 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.

5. MODIFICATIONS

The terms of the Contract, including these USAC Terms and Conditions, shall not be modified other than in writing executed by both parties.

6. INVOICES

A. *Where to Submit Invoices.* Contractor shall submit invoices through the CSP method or via the 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 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 purchase order. 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.

B. *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.

C. *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.

D. *Itemization of Invoices.* USAC may require Contractor to re-submit any invoice with a more detailed itemization of charges upon request.

7. FEES AND RATES INCLUSIVE OF ALL CHARGES AND TAXES

All fees and labor rates specified in the Contract include all charges for labeling, packing, packaging, loading, storage, inspection, insurance, profit and applicable federal, state, or local sales, use, or excise taxes.

8. PAYMENT

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 6 of these USAC Terms and Conditions within thirty (30) calendar days of receipt of invoice, provided the Services and/or Deliverables have been delivered and accepted by USAC.

9. ASSIGNMENT, DELEGATION, AND SUBCONTRACTING

Contractor shall not assign, delegate, 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, delegation, or subcontracting. USAC may require information and assurances that the proposed assignee, delegate, or subcontractor has the skills, capacity, qualifications and financial strength to meet all of the obligations under the Contract. An assignment, delegation, or subcontract shall not release Contractor of the obligations under the Contract, and the assignee, delegate, or subcontractor shall be jointly and severally liable with 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 USAC agrees with Contractor that there is a compelling reason to do so. Contractor shall review the SAM for suspension or debarment status of proposed subcontractors.

10. REPORTS

If any reports are required as part of this Contract, all such reports shall be accurate and timely and submitted in accordance with the due dates specified in this Contract. Should Contractor fail to submit any required reports or correct inaccurate reports, USAC reserves the right to delay payment of invoices until thirty (30) days after an accurate report is received and accepted.

11. TERMINATION FOR CONVENIENCE

USAC may terminate the Contract for any reason or no reason upon one (1) day prior written notice to Contractor without any liability or obligation thereafter. 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 that USAC, in its sole discretion, agrees in writing have resulted directly from the termination.

12. TERMINATION FOR CAUSE

Either party may terminate the Contract for cause upon providing the other party with a written notice. Such notice will provide the other party with a ten (10) day cure period. Upon the expiration of the ten (10) day cure period (during which the defaulting party does not provide a sufficient cure), the non-defaulting party may immediately thereafter terminate the Contract, in whole or in part, if the defaulting party continues to fail to comply with any term or condition of the Contract or fails to provide the non-defaulting 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.

13. STOP WORK ORDER

USAC may, in its sole discretion and without further obligation or liability, 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 in writing, Contractor shall, on the stop work date identified in the stop work or termination notice: (a) stop work, and cause Contractor Personnel 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 USAC Information, Confidential Information, Data, Software, Deliverable, or any Derivative Work to any of the preceding, whether completed or in process, for the work stopped. 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.

14. LIMITATION OF LIABILITY

Except in cases of gross negligence or willful misconduct, in no event shall USAC 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, 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 aggregate amount

paid by USAC to Contractor in the year preceding the most recent of such claims. 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.

15. INDEMNITY

Contractor shall indemnify, hold harmless and defend USAC and its directors, officers, employees and agents against any and all demands, claims and liability, costs and expenses (including attorney's fees and court costs), directly or indirectly related to: (a) any claims or demand for actual or alleged direct or contributory infringement of, or inducement to infringe, or misappropriation of, any intellectual property, including, but not limited to, trade secret, patent, trademark, service mark, or copyright, arising out of or related to Contractor's performance of the Contract; (b) any claims or demands for personal injuries, death or damage to tangible personal or real property to the extent caused by the intentional, reckless, or negligent acts or omissions of Contractor or Contractor Personnel in connection with this Contract; and (c) any claims or demand of any nature whatsoever to the extent caused by violation of these USAC Terms and Conditions by Contractor or Contractor Personnel; (d) any breach of applicable law as described in Section 32 of these USAC Terms and Conditions by Contractor or Contractor Personnel; or (e) the negligence, reckless, illegal, or intentional acts or omissions of Contractor or Contractor Personnel in connection with the performance of the Services.

16. CONFIDENTIAL INFORMATION

A. *Confidential Information.* Confidential Information includes, but is not limited to, USAC Information, Data, materials, or communications in any form or format, whether tangible or intangible, spoken or written (regardless of media) 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;

6. PII; and

7. Information that Recipient knows or reasonably should have known is confidential, proprietary, or privileged.

B. *Non-Disclosure/Use/Irreparable Harm*. It is anticipated that a Discloser may disclose, or has disclosed, Confidential Information to the 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. *Sub-Recipient Access to Confidential Information*. Recipient shall not disclose Confidential Information to a 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 Contractor Personnel to sign a non-disclosure or confidentiality agreement containing terms no less restrictive than those set forth herein. Discloser 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 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 Confidential Information.

E. *Exclusions*. If requested to disclose Confidential Information by an authorized governmental or judicial body, Recipient must promptly notify Discloser of the request and to the extent that it may legally do so, Recipient must refrain from disclosure of the Confidential Information until Discloser 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 immediately notify USAC, with a copy to USAC's General Counsel, of the request. Neither Contractor nor Contractor Personnel 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.

17. RETURN OR DESTRUCTION OF USAC INFORMATION

A. *Return or Destruction of USAC Information.* Except as provided in Section 17.B of these USAC Terms and Conditions, and 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 or Contractor Personnel. If USAC directs that Contractor destroy any USAC Information, then, at USAC's request, Contractor shall provide USAC with an executed certificate in writing stating that all such USAC Information was destroyed.

B. *Federal System of Record.* Contractor acknowledges and agrees that certain USAC Information and Data, may be included in a federal system of record and is subject to record retention schedules set forth by NARA and USAC's records retention policy. Upon expiration or termination of the Contract, information subject to NARA's schedules or USAC's records retention policy shall not be destroyed by Contractor without the written consent of USAC. Contractor will work with USAC in good faith to promptly return all such USAC Information and Data to USAC.

C. *No Withholding of USAC* Information. 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.

D. *Destruction of Hard Copies.* If Contractor destroys hard copies of USAC Information, Contractor must do so by burning, pulping, shredding, macerating, or other means if authorized by USAC in writing.

E. *Destruction of Electronic Copies.* If Contractor destroys electronic copies in computer memory or any other type of media, destruction must be done pursuant to guidelines in NIST SP 800-88 Rev. 1 or the most current revision.

F. *No Other Use.* 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, modified, decompiled, reverse engineered, or commercially exploited by or on behalf of Contractor, Contractor Personnel, or any third party.

18. INFORMATION SECURITY

A. *Data Security Laws.* Contractor shall comply with FISMA, 44 U.S.C. § 3541, et seq., the Privacy Act of 1974 (5 U.S.C. § 552a) as amended (as may be applicable), and NIST SP 800-53 Rev 5. Contractor shall protect PII in accordance with all federal and USAC requirements, including, but not limited to, OMB Memoranda M-17-12 and guidance from NIST including, but not limited to, NIST SP 800-53 Rev 5 and the most current revision of NIST SP 800-61 Rev 2, and FIPS 140-3. Contractor shall cooperate with USAC to implement the abovementioned and any federally mandated information security and privacy requirements not described herein (collectively with the aforementioned laws, regulations, requirements, memoranda and guidance, the "Data Security Laws"). For any Contractor Owned / Controlled IT cloud-based Service that accesses, stores, or otherwise processes USAC Information, USAC Confidential Information, Data, and/or PII, Contractor shall provide documentation and proof of FedRAMP Authorized Designation for use at a moderate risk before any such cloud-based Service may be used. USAC reserves the right to inspect the Authority to Operate notice certified by the Joint Accreditation Board for FedRAMP or the complete package of documents for those with agency accreditation.

B. *Compliance.* Throughout the Contract Term, Contractor shall comply with: (i) USAC's information privacy and IT security policies; and (ii) the prevailing standards of care and best practices regarding information privacy and IT security to the extent they meet or exceed the requirements of the Data Security Laws, the aforementioned USAC policies, or the obligations set forth in these USAC Terms and Conditions.

C. *Compliance Plan*. In providing the Services, Contractor shall conduct itself in a manner that safeguards USAC Data against destruction, loss, damage, corruption, alteration, loss of integrity, commingling, or unauthorized access or processing, which shall be no less rigorous than the most protective of: (a) the requirements of applicable law; (b) the specific standards set forth in this Section 18. Each Party shall designate an individual responsible for coordinating data security related matters for such Party ("Data Security Liaison"), who will be the primary contact person of such Party for all data security related matters under this Terms. In the event a direct interconnection is to be established between Contractor Owned / Controlled IT and USAC IT Systems, the Data Security Liaisons shall execute an interconnection security agreement prior to the establishment of such direct interconnection. Contractor will periodically update and test the Privacy Compliance Plan every calendar quarter.

D. *Integration.* Prior to delivering the Services/Deliverables or enabling data-sharing or interoperability of any kind with USAC's IT System, Contractor shall: (i) work with USAC to document, establish and enable the effective and secure integration of any gateways or data transmission mechanisms necessary for the parties to perform their obligations under the Data Security Laws; (ii) complete any security questionnaires, IT rules of behavior, certifications, assessments, or workforce training reasonably requested by USAC in a timely manner; and (iii) receive prior written authorization from USAC to access USAC's IT System from USAC. If at any time USAC determines that the establishment of such gateways or data transmission mechanisms is reasonably required to securely access the Services or Deliverables, their establishment shall be at Contractor's sole cost and expense. Under no circumstances shall USAC's written authorization to access its IT System serve as a representation or warranty by USAC that such access is secure or as a waiver of these USAC Terms and Conditions. Failure to satisfy the conditions set forth in subsections (i) – (iii) herein to USAC's reasonable satisfaction shall be considered a material breach of the Contract by Contractor.

E. *Policies and Procedures.* Throughout the Contract Term, Contractor shall establish and maintain appropriate internal policies and procedures regarding: (i) the security of the Services, Deliverables, and Contractor's IT System; and (ii) the permitted use, disclosure, access to, and security of PII, Data, USAC Information, USAC Confidential Information, and USAC IT Systems. Contractor shall provide USAC upon request with copies of its information privacy and IT security policies and procedures to review. Such policies and procedures shall not materially conflict with USAC's policies and procedures either expressly or by omission. Contractor agrees to maintain strict control of Contractor's IT System and the access information (e.g. name, username, password, access rights) of all Contractor Personnel to immediately remove access for persons no longer authorized, and to inform USAC immediately if Contractor suspects, or reasonably should expect, there is unauthorized access to USAC's information or IT System. Contractor shall require Contractor Personnel to use Multifactor Authentication. Contractor agrees to require all who access to USAC IT Systems through Contractor to maintain the confidential nature of the USAC Confidential Information, and to not use or access USAC IT Systems except for the benefit of USAC.

F. *Access to PII, Data, USAC Information, USAC Confidential Information and USAC IT Systems.* Contractor agrees that access to the PII, Data, USAC Information, USAC Confidential Information, and USAC's IT Systems is at USAC's sole discretion, and that Contractor's access to such system or information may be conditioned, revoked or denied by USAC at any time, for any reason, without any liability whatsoever to USAC. Access to USAC's IT System by Contractor and Contractor Personnel, including any data-sharing or interoperability between USAC and Contractor, shall be for the sole purpose of providing the Services or Deliverables. Contractor agrees that: (i) USAC's IT System is owned solely by USAC; (ii) USAC will monitor the use of USAC's IT System; (iii) neither Contractor nor Contractor Personnel have any expectation of privacy with regard to USAC's IT System; and (iv) all information appearing on USAC's IT System (except

for information publicly disclosed by USAC) will be considered USAC Confidential Information, as defined by these USAC Terms and Conditions. Contractor will not use USAC's IT System except as expressly authorized by USAC. USAC may require that Contractor Personnel use a USAC.org email address when providing Services. Contractor agrees that its use of, and access to, USAC's IT System is completely at its own risk.

G. *Subcontractors.* Contractor agrees to ensure that any subcontractor that accesses, receives, maintains, or transmits PII, Data, USAC Information, USAC Confidential Information, or USAC's IT System agrees to the same restrictions and conditions that apply throughout these USAC Terms and Conditions to Contractor.

H. *Encryption.* Contractor agrees that PII must be encrypted at all times in accordance with FIPS 140-3 standards. This encryption requirement includes both "Data at Rest" (i.e., stored on a hard drive, CD, DVD, thumb drive, etc.) and "Data in Transit" (i.e., via email or other secured electronic means). Any PII that is retained in documents or other physical formats must be stored in a secured location and with limited access. The standard for disposal of PII requires practices that are adequate to protect against unauthorized access or use of the PII, including at minimum adhering to the provisions of Section 17.

I. *Services Performed in the United States.* All Services must be performed within the United States. This requirement is inclusive of: (a) work related to the Services performed by all Contractor Personnel; and (b) storage and/or processing of data and/or other virtual services (such as cloud storage, remote data processing, *etc*.).

J. *Additional Requirements for Services in Contractor Owned / Controlled IT:*

- If Contractor becomes aware that the Services in Contractor Owned /Controlled IT will lose or has lost its respective FedRAMP Authorized Designation, Contractor shall notify USAC within twenty four (24) hours, shall discontinue use of such Services, and initiate activities to replace the Services that has lost FedRAMP Authorized Designation. Contractor and USAC shall work together to identify a replacement solution. A replacement solution must be identified, and approved in writing by USAC within ten (10) business days of the initial FedRAMP Authorized Designation changes notification.

- Contractor shall implement and use Cloud Protocols in connection with the Services operated in cloud infrastructure environments provided and controlled by any third-party. USAC's receipt of the Services, and Contractor's and USAC's use of the Services shall be in accordance with such Cloud Protocols.

- Contractor shall maintain Contractor Owned/Controlled IT used by Contractor in performance of the Services. USAC may require Contractor to respond to the information security questionnaires regarding Contractor's information security policies and practices. USAC will conduct its information security review, if required, with reference to the responses Contractor provides to such information security questionnaires. At USAC's request, Contractor shall also respond promptly (within not more than 10 business days) to any new or supplemental information security questions the USAC may require of Contractor during performance. USAC may terminate the Contract upon notice if Contractor fails to provide a timely response to requests for new or supplemental information security information or if USAC determines that Contractor's information security policies or practices increase risk to USAC in a manner unacceptable to USAC.

- Contractor shall maintain administrative, technical, physical, and procedural information security controls compliant with ISO 27001 standards for all Contractor Owned/Controlled IT used by Contractor in performance of the Services. Contractor shall maintain ISO 27001 Compliance certification and notify USAC of any changes to its compliance. Contractor shall provide USAC with its ISO 27001 Compliance certification within ten (10) days of the Effective Date of the Contract.

19. SECURITY INCIDENTS AND DATA BREACHES

A. *Identification and Notification.* Contractor shall identify Security Incidents or Data Breaches and notify USAC at incident@USAC.org and Privacy@USAC.org of any actual or suspected Security Incident or Data Breach within one (1) hour of becoming aware of an actual or suspected Security Incident or Data Breach.

B. *Notice.* Contractor's notice to USAC shall include the following: (i) a description of the Security Incident or Data Breach, including the date of the Security Incident or Data Breach, including the date of discovery by Contractor, if known; (ii) a description of the type(s) of Malicious Code, PII, Data, USAC Information, USAC Confidential Information, or USAC IT System involved in the Security Incident or Data Breach, if any; (iii) to the extent possible, a list of each individual whose PII has been, or is reasonably believed to have been accessed, acquired, used or disclosed during or as a result of the Security Breach or Data Breach; (iv) a brief description of what Contractor is doing to investigate the Security Incident or Data Breach and mitigate the harm to USAC; (v) any steps Contractor recommends USAC should take a protect itself from potential harm resulting from the Security Breach or Data Breach; (vi) the name, phone number, and e-mail address of Contractor's representative responsible for responding to the Security Incident or Data Breach; and (vii) any information required for USAC to comply with the Data Security Laws. Upon receiving Contractor's initial notice, USAC shall have the right to immediately take any security measures it deems reasonably

necessary to mitigate the harmful effects to the PII, Data, USAC Information USAC Confidential Information, or the USAC IT Systems. Contractor will regularly supplement its notice(s) with additional information as it becomes available.

C. *Mitigation and Elimination Efforts.* Contractor, working with USAC, shall use its best efforts to mitigate and eliminate the effects of the Security Incident or Data Breach on USAC and, if the Security Incident or Data Breach causes any loss of operational efficiency, loss of data, or unauthorized disclosure, Contractor will assist USAC in mitigating or restoring such losses or disclosures. Contractor agrees to fully cooperate with USAC in the investigation of the Security Incident or Data Breach and to participate in, to the extent directed by USAC, the notification of individuals, the media, the FCC, or third parties. Contractor shall promptly respond to USAC's questions regarding the Security Incident or Data Breach and coordinate with Contractor Personnel if required to mitigate the harm. To the extent USAC determines necessary, USAC agrees to provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. Notwithstanding anything to the contrary in the Contract, if the Security Incident or Data Breach is due to the negligence or misconduct of Contractor or Contractor Personnel, then Contractor shall: (i) perform its obligations under this Section at no cost to USAC; (ii) promptly implement or develop any additional protocols, policies, gateways, transmission mechanisms, or security layers, if reasonably necessary, at its sole cost and expense, and with the approval of USAC; (iii) indemnify USAC for all damages, and if needed PII, USAC Information, USAC Confidential Information, Data, and USAC IT Systems breach mitigations, under this Section as a result of the Security Incident or Data Breach. Failure to strictly abide by these USAC Terms and Conditions shall be considered a material breach of the Contract for which USAC shall have the right to immediately terminate for cause.

D. *Backups*. Contractor shall make reasonable backups of all USAC Information and shall ensure that the Services allow for the automatic backup of USAC Information in Contractor Owned / Controlled IT.

E. *Security Audits.* USAC or its designee may, at USAC's expense and at any time, perform an audit of the security policies and procedures implemented by Contractor and in effect at for Contractor Owned / Controlled IT and the physical locations where such environments are housed or may be accessed.

F. *Cooperation.* Contractor will cooperate with USAC in any litigation and investigation against third parties deemed necessary by USAC to protect USAC Information, Data, USAC Confidential Information, PII and USAC IT Systems. Each Party will bear the costs it incurs as a result of compliance with this Section.

20. MALICIOUS CODE AND MALICIOUS CYBER ACTIVITIES

USAC may provide Contractor access to one or more of the USAC IT Systems. Contractor agrees that the USAC IT Systems are owned by USAC, that USAC reserves the right to monitor use of the USAC IT Systems, that neither Contractor nor Contractor Personnel should have any expectation of privacy with regard to use of the USAC IT Systems, and that all information appearing on the USAC IT Systems (except for authorized information provided by Contractor or information publicly disclosed by USAC) will be considered as USAC Confidential Information. Contractor agrees that it will not use the USAC IT Systems except as expressly authorized by USAC in this Contract. Contractor agrees to maintain strict control of all usernames, passwords and access lists it is given to the USAC IT Systems for of Contractor Personnel as are necessary to perform under this Contract, to immediately remove such access for those persons no longer authorized, and to inform USAC immediately if there is reason to believe there is unauthorized access. Contractor agrees to cause all who gain access to the USAC IT Systems through Contractor to maintain the confidential nature of all Confidential Information, and to not use the USAC IT Systems except for the benefit of USAC. Contractor agrees that it will use the USAC IT Systems completely at its own risk, and that it will be liable to USAC for any damages incurred by USAC as a result of Contractor's violation of this Section.

Contractor will not introduce Malicious Code into USAC IT Systems or engage in Malicious Cyber Activities in, with, or involving the Services or USAC IT Systems. For any aspect of the Services in Contractor's IT Systems, Contractor will comply with NIST SP 800-83 Rev. 1 or the most current revision thereof to prevent Malicious Code. Contractor will perform regularly scheduled (preferably in real-time, but in no event less frequently than daily) virus checks using the latest commercially available, most comprehensive virus detection and scanning programs. If Contractor becomes aware that any Malicious Code has been introduced into any USAC IT System, or that Contractor has engaged in Malicious Cyber Activities, Contractor will notify USAC immediately. In addition, Contractor will use its best efforts to assist USAC in reducing the effects of the Malicious Code or Malicious Cyber Activities and, if the Malicious Code or Malicious Cyber Activity causes a loss of operational efficiency or loss of data, to assist USAC in mitigating and restoring such losses. USAC will provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. If Malicious Code is found to have been introduced into any USAC IT System or the Services, Contractor will perform all of its obligations under this Section at no cost to USAC, and Contractor will be liable to USAC for damages and costs incurred by USAC as a result of such Malicious Code. If Contractor or Contractor Personnel has been found to (a) have engaged in any Malicious Cyber Activities; or (b) have allowed Malicious Cyber Activities to have occurred due to its willful, reckless, or negligent actions or omissions, Contractor will be liable to USAC for damages and costs incurred by USAC as a result of such Malicious Cyber Activities.

The introduction of Malicious Code into USAC's IT System, and/or the engaging in Malicious Cyber Activity involving USAC IT Systems, shall be considered a Data Breach. If Contractor becomes aware that Malicious Code has been introduced into USAC IT Systems, or Contractor has engaged in Malicious Cyber Activity, Contractor will notify USAC immediately in writing within the time frame required by the United States Computer Emergency Readiness Team and

FCC, which is currently within one (1) hour and otherwise act in a manner consistent with Section 19 of these USAC Terms and Conditions.

21. FISMA PROVISIONS

Contractor shall meet and comply with all USAC IT security policies and all applicable USAC and other laws and regulations for the protection and security of information systems and Data (including but not limited to FISMA, OMB, and NIST requirements). At its sole discretion, USAC may revise any USAC IT security policy at any time.

Safeguarding of Contractor IT Systems:

USAC's security strategy for Data includes the requirement to ensure the security of protection controls for Data regardless of the location or the party responsible for those controls. Contractor acknowledges that it serves a vital role in achieving this goal. Contractor shall apply the following minimum safeguarding requirements and procedures from NIST SP 800-171 Revision 2 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" to protect covered Contractor IT Systems and USAC Data. Contractor shall, upon request, provide USAC with copies of its security policies and procedures to review. USAC may require a written response that may be an attestation of compliance, a submission of supporting document, or both. If USAC requests such a written response, Contractor shall submit an electronic copy of the document(s) confirming compliance within ten (10) calendar days. If there are any requirements that are out of scope or that cannot be complied with, Contractor shall fully explain those requirements with a business justification to USAC. Contractor must be in compliance with all such requirements unless USAC agrees in writing with Contractor that Contractor does not have to comply. If Contractor is not in compliance with all requirements and has not received written confirmation from USAC that Contractor may not comply with a requirement, USAC may terminate this Contract immediately upon written notice to Contractor.

Contractor shall:

1. Limit Contractor IT Systems access to only authorized USAC employees and contractors, authorized Contractor Personnel and authorized processes.
2. Limit Contractor IT Systems access to only the types of transactions and functions that USAC employees and contractors and authorized Contractor Personnel are permitted to execute.
3. Verify and control/limit connections to and use of external Contactor IT Systems.
4. Control information posted or processed on publicly accessible Contractor IT Systems.
5. Sanitize or destroy Contractor IT Systems media containing USAC Information as described in Section 17.C. of these USAC Terms and Conditions.
6. Limit physical access to Contractor IT Systems, equipment, and the respective operating environments to only USAC employees and contractors and authorized Contractor Personnel.

7. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
8. Monitor, control, and protect Contractor organizational communications (i.e., information transmitted or received by Contractor IT Systems) at the external boundaries and key internal boundaries of the Contractor IT Systems.
9. Implement subnetworks for publicly accessible Contractor IT Systems components that are physically or logically separated from internal networks.
10. Identify, report, and correct information and Contractor IT Systems flaws promptly.
11. Provide protection from Malicious Code at appropriate locations within Contractor IT Systems.
12. Update Malicious Code protection mechanisms when new releases are available.
13. Perform periodic scans (no less frequently than daily) of Contractor's IT Systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

22. TECHNOLOGY CONSIDERATIONS

Contractor shall ensure that COTS, SaaS, PaaS, or IaaS Software deployed in Contractor Owned / Controlled IT cloud or on USAC's Amazon Web Services GovCloud infrastructure satisfies the following requirements:

A. The Software must be able to utilize USAC's instance of OKTA's Identity and Access Management software for user authentication and provisioning. OKTA is a cloud-based Identity and Access Management product used by USAC.

B. Any USAC Data stored in a COTS/SaaS/PaaS/IaaS database must be readily accessed by USAC in a format determined at USAC's sole discretion via standard web services or another standard access mechanism.

C. Any COTS, SaaS, PaaS, or IaaS Software must have either: (1) an Authority to Operate issued by a federal agency along with the FedRAMP-Authorized Designation issued by the FedRAMP Project Management Office, or (2) a Joint Authorization Board issued Authority to Operate along with the FedRAMP-Authorized Designation issued by the FedRAMP Project Management Office. Furthermore, any COTS, SaaS, PaaS, or IaaS Software must maintain the FedRAMP-Authorized Designation for the Contract Term.

Contractor shall ensure that any Software developed and/or deployed for USAC:

A. Meets all USAC architecture, standards, and IT security guidelines and standards. This includes, but is not limited to, the ability to achieve an Authority to Operate based on all applicable OMB, NIST, and FISMA guidelines.

B. Reuses available USAC technology services (microservices, APIs) unless Contractor demonstrates in writing that those services are unable to meet the requirements and USAC agrees to the substitute solution in writing with Contractor.

C. Uses the USAC technical stack unless Contractor demonstrates in writing that those components are unable to meet the requirements and USAC agrees in writing with Contractor. Key components of USAC's technical stack include the following:

- Java / Spring Framework Suite (Language and frameworks)
- OKTA (Identity and Access Management)
- Apache Kafka (Messaging)
- PostgreSQL / PostGIS (Database)
- Elasticsearch, Logstash, Kibana
- Atlassian tools (SDLC)
- Apache Tomcat (Application Servers)
- Red Hat Enterprise Linux (OS)

Further details of USAC's technical stack and service architecture may be provided as appropriate.

23. PROPRIETARY RIGHTS

Contractor agrees that all Data, Software, Deliverables, and all Derivative Works thereof are USAC property and shall be deemed USAC Information and are works made-for-hire for USAC within the meaning of the copyright laws of the United States. In the event that any of the aforementioned are not considered works made-for-hire for USAC within the meaning of the copyright laws of the United States, Contractor shall and hereby does irrevocably grant, assign, transfer and set over unto USAC in perpetuity all worldwide rights, title and interest of any kind, nature or description it has or may have in the future in and to such materials, and Contractor shall not be entitled to make any use of such materials beyond what may be described in this Contract. Contractor hereby waives, and shall secure waiver from Contractor Personnel any moral rights in such assigned materials, such as the right to be named as author, the right to modify, the right to prevent mutilation and the right to prevent commercial exploitation. Accordingly, USAC shall be the sole and exclusive owner for all purposes for the worldwide 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.

USAC may assign to the FCC any intellectual property rights USAC may have to any Data, Software, Deliverables, USAC Information and all Derivative Works thereof without notice to, or prior consent of, Contractor.

Nothing in this Contract shall be deemed to imply the grant of a license in or transfer of ownership or other rights in the Data, Software, Deliverables, USAC Information and all Derivative Works thereof, and Contractor acknowledges and agrees that it does not acquire any of the same, except to provide Services to USAC as expressly set forth in this Contract.

Contractor shall not, without the prior written permission of the USAC, incorporate any Data, Software, Deliverable, or any Derivative Work thereof delivered under the Contract not first produced in the performance of the Contract unless Contractor: (a) identifies the Data, Software, Deliverable, and any Derivative Work thereof; and (b) grants to USAC, or acquires on USAC's behalf, a perpetual, worldwide, royalty-free, non-exclusive, transferable license to use and modify such Data, Software, Deliverable, and any Derivative Work thereof in any way.

24. 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 Contractor Personnel, including any actions that violate law, are negligent, or that constitute a breach of the Visitor Form and/or the Contract.

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 before being given access to USAC IT Systems. Contractor may be required to complete Role-Based Privacy Act Training, at Contractor's own cost, if accessing USAC information systems designated as federal systems of record.

Security Briefings. Before receiving access to IT resources under the Contract, Contractor personnel must provide security training to Contractor Personnel. USAC will review and approve Contractor's security training materials (including any security training materials in the event such training is provided to Contractor by any subcontractors, consultants, or agents) and verify that training certifications and records are provided, if requested during an annual FISMA audit. If Contractor Personnel will be in USAC offices or have access to USAC IT systems, background checks are required pursuant to NIST. Contractor shall conduct background checks on Contractor Personnel and provide evidence of the background checks to USAC upon request.

25. KEY PERSONNEL

USAC may specify which Contractor employees are Key Personnel under the Contract. Key Personnel assigned to the Contract must remain in their respective positions throughout the Contract Term. USAC may terminate all or a part of the Contract if 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:

A. 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

B. 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 shall apply to their placement on and removal from the Contract.

26. SHIPMENT/DELIVERY

Terms of any shipping are F.O.B. USAC's delivery location unless otherwise noted in the Contract. All goods, products items, materials, etc. purchased hereunder must be packed and packaged to ensure safe delivery in accordance with recognized industry-standard commercial practices. If, in order to comply with the applicable delivery date, Contractor must ship by a more expensive means than that specified in the Contract, Contractor shall bear the increased transportation costs resulting therefrom unless the necessity for such shipment change has been caused by USAC. If any Deliverable is not delivered by the date specified herein, USAC reserves the right, without liability, to cancel the Contract as to any Deliverable not yet shipped or tendered, and to purchase substitute materials and to charge Contractor for any loss incurred. Contractor shall notify USAC in writing promptly of any actual or potential delays (however caused) which may delay the timely performance of this Contract. If Contractor is unable to complete performance at the time specified for delivery hereunder, by reason of causes beyond Contractor's reasonable control, USAC may elect to take delivery of materials in an unfinished state and to pay such proportion of the Contract price as the work then completed bears to the total work hereunder and to terminate this Contract without liability as to the balance of the materials covered hereunder.

27. 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 claims, risks and damages/injuries that may arise under the Contract, including, as appropriate, worker's compensation, employer's liability, commercial general liability, commercial crime coverage, automobile liability, professional liability, cyber liability (which may be included in some professional liability coverage), and excess / umbrella insurance. Upon USAC's request, Contractor shall name USAC as an additional insured to those insurance policies that allow it. Upon USAC's request, Contractor shall cause its insurers to waive their rights of subrogation against USAC. Contractor shall produce evidence of such insurance upon request by USAC. If the insurance coverage is provided on a claims-made basis, then it must be maintained for a period of not less than three (3) years after acceptance of the Deliverables and/or Services provided in connection with this Contract. Contractor shall provide written notice thirty (30) days prior to USAC in the event of cancellation of or material change in the policy.

Contractor shall be liable to USAC for all damages incurred by USAC as a result of Contractor's failure to maintain the required coverages with respect to its subcontractors, or Contractor's failure to require its subcontractors to maintain the coverages required herein.

28. 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 organizational or personal 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 maintain written standards of conduct covering conflicts of interest and provide a copy to USAC upon USAC's request. Contractor shall promptly notify 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 promptly of any conflicts Contractor has with USAC vendors. Failure to provide adequate means to avoid, neutralize or remediate any conflict of interest may be the basis for termination of the Contract. By its execution hereof, 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 government employee in connection with the award. In order to maintain the absence of an actual or apparent conflict of interest as described herein, Contractor must not advocate any policy positions with respect to the USF programs or the USF during the term of the Contract. 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.

29. WAIVER

Any waiver of any provision of this Contract must be in writing and signed by the parties hereto. Any waiver by either party of a breach of any provision of this Contract by the other party shall not operate or be construed as a waiver of any subsequent breach by the other party.

30. 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. 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.

31. CHOICE OF LAW / CONSENT TO JURISDICTION

The Contract shall be governed by and construed in accordance with the laws of the District of Columbia 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 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 procurement specialist and USAC General Counsel for informal resolution prior to initiating any action in the Courts and must work with USAC in good faith to resolve any disputed issues. If any disputed issue by Contractor is not resolved after thirty (30) calendar days of good faith attempts to resolve it, Contractor may instigate legal proceedings. 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.

32. USAC AND APPLICABLE LAWS

USAC is not a federal agency, a government corporation, a government controlled corporation or any 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 the Procurement Regulations. Contractor shall comply with the Procurement Regulations and all applicable federal, state and local laws, executive orders, rules, regulations, declarations, decrees, directives, legislative enactments, orders, ordinances, common law, guidance, or other binding restriction or requirement of or by any governmental authority related to the Services or Contractor's performance of its obligations under this Contract, and includes without limitation FCC Orders; the rules, regulations and policies of the FCC; the Privacy Act of 1974; FISMA; NIST guidelines which provide the requirements that the federal government must follow regarding use, treatment, and safeguarding of data; and OMB Guidelines pertaining to privacy, information security, and computer matching; the Communications Act of 1934; and the Communications Act of 1996.

33. 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 Code, licenses to rights to "intellectual property" as defined in the Code. The parties agree that USAC, as licensee of such rights under 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 Data, Software, Deliverable, or any Derivative Work thereof.

34. NON EXCLUSIVITY

Except as may be set forth in the Contract, 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 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.

35. INDEPENDENT CONTRACTOR

Contractor acknowledges and agrees that it is an independent contractor to USAC and Contractor Personnel 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 Personnel. 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.

36. TEMPORARY EXTENSION OF SERVICES

USAC may require continued performance of any Services within the limits and at the rates specified in the Contract. Except as may be set forth in the Contract, USAC may extend the Services more than once, but the total extension of performance hereunder shall not exceed six (6) months. USAC may exercise an option to extend by written notice to Contractor within ten (10) days prior to expiration of the then current Initial Term or Optional Renewal Term.

37. 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:
Chief Administrative Officer, Universal Service Administrative Company

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.

With a copy to:

General Counsel, Universal Service Administrative Company
700 12th Street, NW, Suite 900
Washington, DC 20005
Email: OGCContracts@usac.org

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

38. 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.

39. FORCE MAJEURE

Neither party to this Contract is liable for any delays or failures in its performance hereunder resulting from circumstances or causes beyond its reasonable control, including, without limitation, force majeure acts of God (but excluding weather conditions regardless of severity), fires, accidents, epidemics, pandemics, riots, strikes, acts or threatened acts of terrorism, war or other violence, or any law, order or requirement of any governmental agency or authority (but excluding orders or requirements pertaining to tax liability). Upon the occurrence of a force majeure event, the non-performing party shall provide immediate notice to the other party and will be excused from any further performance of its obligations effected by the force majeure event for so long as the event continues and such party continues to use commercially reasonable efforts to resume performance as soon as reasonably practicable, and takes reasonable steps to mitigate the impact on the other party. If such non-performance continues for more than ten (10) days, then the other party may terminate this Contract with at least one (1) day prior written notice to the other party. In the event that the force majeure event is a law, order, or requirement made by a government agency or authority related to USAC and the purposes of this Contract, USAC may immediately terminate this Contract without penalty upon written notification to Contractor.

40. 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.

41. SECTION 508 STANDARDS

Compliance with Section 508. Contractor shall ensure that Services provided under the Contract comply with the applicable electronic and information technology accessibility standards established in 36 C.F.R. Part 1194, which implements Section 508 of the Rehabilitation Act, 29 U.S.C. § 794d.

TDD/TTY Users. Contractor shall ensure that TDD/TTY users are offered similar levels of service that are received by telephone users supported by the Contract. Contractor shall also ensure that the Services provided under the Contract comply with the applicable requirements of 18 U.S.C. § 2511 and any applicable state wiretapping laws.

42. NATIONAL SECURITY SUPPLY CHAIN REQUIREMENTS

A. *Definitions.* For purposes of this Section, the following terms are defined as stated below:

1. "Covered Company" is defined as an entity, including its parents, affiliates, or subsidiaries, finally designated by the Public Safety and Homeland Security Bureau of the FCC as posing a national security threat to the integrity of communications networks or the communications supply chain.
2. "Covered Equipment or Services" is defined as equipment or services included on the FCC-issued Covered List that pose a national security threat to the integrity to the communications supply chain.
3. "Covered List" is a list of covered communications equipment and services that pose an unacceptable risk to the national security of the United States. The FCC may update the list at any time. The list can be found at fcc.gov/supplychain/coveredlist.
4. "Reasonable Inquiry" is defined as an inquiry designed to uncover information about the identity of the producer or provider of equipment and services that has been purchased, obtained, maintained, or otherwise supported by funds from USAC under this Contract.

B. *Prohibition*. Contractor will ensure that no funds from USAC or other federal subsidies under this Contract will be used to purchase, obtain, maintain, or otherwise support any

equipment or services produced or provided by a Covered Company. Contractor must also ensure that no funds administered by USAC or the FCC under this Contract will be used to purchase, obtain, maintain or otherwise support Covered Equipment or Services placed on the Covered List. These prohibitions extend to any subcontractors that provides Services under the Contract. Contractor is responsible for notifying any subcontractors it engages under this Contract of this prohibition.

C. *Monitoring*. Contractor must actively monitor what entities have been finally designated by the FCC as a Covered Company and what equipment and services the FCC defines as Covered Equipment or Services and places on the Covered List. Contractor must actively monitor to ensure that no funds from USAC or other federal subsidies are used to purchase, obtain, maintain, or otherwise support any equipment or services produced or provided by a Covered Company from Contactor or any subcontractor it engages under the Contract. Contractor must also ensure that no funds administered by USAC or other federal subsidies are used to purchase, obtain, maintain, or otherwise support any Covered Equipment or Services that the FCC has placed on the Covered List from Contractor or any subcontractor it engages under the Contract. If Contractor finds that they have violated any or all of these prohibitions, then, Contractor shall immediately notify USAC. In Contractor's notification to USAC, Contractor shall provide the same information required for non-compliance in Section 42.D of these USAC Terms and Conditions. Any such notification must have audit ready supporting evidence.

D. *Annual Certification*. Contractor will conduct a Reasonable Inquiry and provide a certification to USAC in writing upon execution of this Contract and no later than December 31 of each calendar year that the Contract is in effect. If Contractor, and all applicable subcontractors, are in compliance with Section 42.B. of these USAC Terms and Conditions, Contractor shall state in the annual certification that no funds from USAC have been used to purchase, obtain, maintain, or otherwise support any equipment or services produced or provided by a Covered Company or Covered Equipment or Services on the Covered List. If Contractor, or any applicable subcontractor, is not in compliance with Section 42.B. of these USAC Terms and Conditions, Contractor shall so inform USAC and provide the following information in the certification:

(i) If for equipment produced or provided by a Covered Company or equipment on the Covered List:
   a. The Covered Company that produced the equipment (include entity name, unique entity identifier, CAGE code, and whether the Covered Company was the original equipment manufacturer ("OEM") or a distributor, if known);
   b. A description of all equipment (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

c. Explanation of the why USAC funds purchased, obtained, maintained, or otherwise supported the equipment and a plan to remove and replace such equipment as expeditiously as possible.

(ii) If for services produced or provided by a Covered Company or services on the Covered List:

a. If the service is related to item maintenance: A description of all such services provided (include on the item being maintained: brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable);
b. If the service is not associated with maintenance, the product service code of the service being provided; and
c. Explanation of the why USAC funds purchased, obtained, maintained, or otherwise supported the services and a plan to remove and replace such service as expeditiously as possible.

Contractor shall retain audit ready supporting evidence for all certifications.

43. ADDED SERVICES

USAC may at any time submit a request that Contractor perform any Added Services. Before Contractor performs an Added Services, USAC and Contractor must execute an amendment to this Contract that, at a minimum, will provide: (a) a detailed description of the services, functions and responsibilities of the Added Service; (b) a schedule for commencement and completion of the Added Services; (c) a detailed breakdown of Contractor's fees for the Added Services; (d) a description of any new staffing and equipment to be provided by Contractor to perform the Added Services; and (e) such other information as may be requested by USAC.

44. ADEQUATE COVID-19 SAFETY PROTOCOLS

To provide adequate COVID-19 safeguards for USAC employees, Contractor shall ensure that Contractor Personnel that enter USAC premises comply with all guidance for Contractor or subcontractor workplace locations published by the Safer Federal Workforce Task Force ("Guidance") for the duration of the Contract.

Nothing in this Section shall excuse noncompliance with any applicable federal, state and local laws establishing more protective safety protocols than those established under the Guidance.

SECTION D:
Attachments

Attachment List:

- Attachment 1 - Bid Sheet
- Attachment 2 - [Place Holder]
- Attachment 3 - Confidentiality Agreement

SECTION E:
Instructions and Evaluation Criteria

1. 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 may 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** to the proposal, "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. 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.7. Statement of Work, 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 **March 7, 2022** ("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-22-012, of this RFP.

C. PROPOSAL SCHEDULE

DATE	EVENT
February 4, 2022	RFP Released
February 14, 2022	Questions Due to USAC by 11:00 AM ET at rfp@usac.org
February 18, 2022	Answers posted by USAC
March 7, 2022	Proposal Due to USAC by 11:00 AM ET at rfp@usac.org
March 23-24, 2022*	Potential date for oral demonstrations
March 29, 2022*	Final Proposal Revisions due
April 2022*	Anticipated Award Date
May 2022*	Work Begins

*Dates are subject to change at USAC's sole discertion.

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.

2. 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.

3. 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.16.

4. 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,
- 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.

5. PROPOSAL CONTENT

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

Volume 1 - Corporate Information

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 the Executive Summary.

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.

Volume 2 – Technical

This volume must include:

1. A cover page, as outlined above.

2. A summary detailing Offeror's FISMA and NIST security framework and organization information security support.

3. An in-depth discussion of Offeror's technical approach to providing the services listed in Section B.7., along with a clear statement of whether or not the Offeror's performance of the Contract will comply with all requirements stated in this RFP, and the USAC Terms and Conditions set forth in Section C. Offerors must submit a detailed response to this RFP. The Offeror must clearly state whether it will comply with all requirements stated in this RFP, and the USAC Terms and Conditions set forth in Section C, and provide detailed information about how it will fulfill the requirements of the RFP. Any deviations from, or exceptions to, the requirements in this RFP the or USAC Terms or Conditions set forth in Section C must be clearly identified in an Attachment to the proposal.

   Note: Offers that include material deviations from, or take material exceptions to, RFP requirements, USAC 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 Offeror "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 Offeror'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 USAC's Information Security Program, including how the Offeror intends to staff and complete these activities. ~~Offerors shall describe in detail their plan for completing the Digital government consulting identified in Section B.VIII in a time allotted.~~ If Offeror currently has staff or personnel who meet the qualifications for the services identified in Section B.7., and who are available for assignment under an awarded contract, please provide a resume (not to exceed two (2) pages) that includes their educational background, job and related experience, and the specific position(s) for which they are available on the Contract.

    a. Offeror shall provide an Information Security Program Plan Framework that highlights their expertise in conducting these type of consulting services. The Contractor's responses associated with the Information Security Program Plan Framework will be an inherent part of the evaluation conducted by USAC.

7. Experience. Describe your firm's experience with consultation and support of an organization's information security program of similar size and scope. Provide examples of the projects and personnel to include types of positions and length of assignments.

8. Key Personnel. Identify by name all key personnel. Describe the technical knowledge of 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. 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. Submit resumes for all key personnel, as an attachment (**Attachment A**) to the technical volume, no longer than two (2) pages in length per resume.

b. If Offeror, at 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 Offeror, Offeror shall identify such personnel and include the expected termination date in the proposal.

Volume 3 – Past Performance

This volume must include:

1. A cover page, as outlined above.

2. A list of up to three (3) current or recently completed contracts for similar in scope to those required by this solicitation. Each entry on the list must contain: (i) the client's name, (ii) the project title, (iii) the period of performance, (iv) the contract number, (v) the contract value, (vi) a primary point of contact (including the telephone number and email address for each point of contact, if available), and (vii) 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, and (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.

Volume 4 – Price

This volume must include:

1. A cover page, as outlined above.

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

    a. The fixed information security program management activities prices should be *fully loaded* and must include wages, overhead, general and administrative expenses, taxes and profit.

Page Count Limits

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

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

2. Volume 2 – Technical; may not exceed twenty (20)~~fifteen (15)~~ pages including Cover page; however excluding **Attachment A** (Resumes)

3. Volume 3 – Past Performance Information; may not exceed five (5) pages, including Cover page.

4. Volume 4 – Price; may not exceed five (5) pages, including Cover page.

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

6. 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.

1. **Technical:** The technical sub-factors listed below in descending order of importance:
    a. Technical Approach
    b. Timeline, including Information Security Program Draft Plan
    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, decency and quality of the Offeror's past performance on past or current contracts for the same or similar services. 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 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.