



USAC Solicitation for Chief Information Security Officer Advisory Services

SOLICITATION INFORMATION:

Method of Solicitation: Request for Proposal (“RFP”)
 Contract Period of Performance: One (1) year base plus three (3) option years
 Solicitation Number: IT-23-053
 Solicitation Issue Date: July 12, 2023
 Question Due Date: July 20, 2023 at 11:00 AM ET
 Offer Due Date: August 15, 2023 at 11:00 AM ET

CONTRACT TO BE ISSUED BY:

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

CONTACT INFORMATION:

USAC CONTACT INFORMATION	OFFEROR CONTACT INFORMATION
Anthony Smith Procurement Specialist Phone: 202-916-3486 Email: Anthony.Smith@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”), the Universal Service Administrative Company (“USAC”) works to promote the availability of quality telecommunications 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, 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 the High Cost Program, Lifeline Program, Rural Health Care Program, and Schools and Libraries Program.

USAC strives to provide efficient, responsible stewardship of the programs, each of which is 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 other divisions, including Finance, Office of General Counsel (“OGC”), Information Systems, Audit and Assurance, Enterprise Process Improvement (“EPI”), and Human Resources (“HR”).

Consistent with FCC rules, USAC does not make policy nor interpret unclear provisions of statutes or the FCC’s rules. The USF is funded by contributions from telecommunications carriers, including wireline and wireless companies, and contributions from interconnected voice over internet protocol (“VoIP”) 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 designed to ensure that consumers in rural, insular, and high-cost areas have access to modern communications networks capable of providing voice and broadband service, both fixed and mobile, at rates that are reasonably comparable to those in urban areas (“High Cost”). High Cost fulfills this universal service goal by allowing eligible carriers who serve these areas to recover some of their costs from the USF. Like all USF programs, the administration of High Cost has undergone significant modernization in the last several years to increase innovation and ensure beneficiaries have access to updated technology. USAC developed and now leverages the High Cost Universal Broadband Portal (“HUBB”), which allows participating carriers 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 displays this information on a public-facing map to show the impact of high-cost funding on broadband expansion throughout the United States.

Lifeline Program

The Lifeline Program provides support for discounts on broadband and voice services to eligible low-income households (“Lifeline”). USAC uses its centralized application system, the Lifeline National Eligibility Verifier (“National Verifier”), to verify consumer eligibility through proof of income or the consumer’s participation in a qualifying federal benefit program, such as Medicaid, the Supplemental Nutritional Assistance Program (“SNAP”), Federal Public Housing Assistance, or Veterans and Survivors Pension Benefit. USAC focuses on metrics and data analytics for Lifeline improvement and provides outreach efforts to eligible households to increase participation in and the effectiveness of Lifeline. USAC also works to ensure program integrity by supporting the needs of Lifeline stakeholders, reducing program inefficiencies, and combating waste, fraud, and abuse. USAC reviews processes regularly to increase compliance, identify avenues for operational improvements, and refine program controls, such as audit processes.

Rural Health Care Program

The Rural Health Care Program supports health care facilities in bringing medical care to rural areas through increased connectivity (“RHC”). RHC consists of two main component programs: (1) the Telecommunications Program (“Telecom”) and (2) the Healthcare Connect Fund Program (“HCF”). The FCC established Telecom in 1997 to subsidize the difference between urban and rural rates for telecommunications services. Under Telecom, eligible rural health care providers can obtain rates on telecommunications services in rural areas that are reasonably comparable to rates charged for similar services in corresponding urban areas. In 2012, the FCC established HCF to promote the use of broadband services and facilitate the formation of health care provider consortia that include both rural and urban health care providers. HCF provides a discount on an array of advanced telecommunications and information services such as Internet access, dark fiber, business data, traditional DSL, and private carriage services. These telecommunications and broadband services support telemedicine by ensuring that health care providers can deliver cutting edge solutions and treatments to Americans residing in rural areas.

Schools and Libraries Program (E-Rate)

The Schools and Libraries Program helps schools and libraries obtain high-speed Internet access and telecommunications services and equipment at affordable rates (“E-Rate”). E-Rate provides a discount for the cost of broadband and telecommunications services to and within schools and libraries in order to support a modern and dynamic learning environment. Applicants and service providers submit FCC Forms (e.g. requests for services or funding) and other compliance-related documentation to the E-Rate Productivity Center (“EPC”), an electronic platform that enables participation in the program. USAC frequently invests in new tools and data analytics capabilities to support the success of the program in alignment with the FCC’s goals.

Contributions

Universal service support is money collected from telecommunications companies and then dedicated to fulfilling the goals of universal service.

Universal service is paid for by contributions from telecommunications carriers, including wireline and wireless companies, and interconnected Voice over Internet Protocol (VoIP) providers, including cable companies that provide voice service, based on an assessment of their interstate and international end-user



revenues. Telecommunications companies are required by law to make contributions to the USF, paying in a percentage of their end-user interstate and international revenues.

All telecommunications companies must register with USAC, whether they contribute to the USF directly or through their underlying carriers. All intrastate, interstate, and international providers of telecommunications (including VoIP providers) within the United States, with limited exceptions, are legally obligated to file the FCC Forms 499.

The term “telecommunications” refers to the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received.

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

2. PURPOSE

USAC is seeking a Contractor to provide the following Chief Information Security Officer (“CISO”) advisory services:

1. Information Security Program (as described in more detail in Section B.1., third paragraph and bullets thereunder of this RFP and Section B.7.A. of this RFP -- “Information Security Program”) management support.
2. Collective Incident Response preparedness and training (as described in more detail in Section B.7.B of this RFP -- “Incident Response”) support.
3. Information Security Awareness Training Support (as described in more detail in Section B.7.C. -- “Information Security Awareness Training Support”).
4. Information Technology, Information Security, and Cybersecurity Audit Support (as described in more detail in Section B.7.D -- “Information Technology, Information Security, and Cybersecurity Audit Support”).

Any party that provides a bid and proposal to this RFP is considered an “Offeror”. Any Offeror that is awarded work under this RFP and enters into a contract with USAC to deliver the awarded work is considered a “Contractor”.

3. CONFIDENTIALITY

This RFP 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. Any contract for awarded work under this RFP will also be subject to the terms of such Confidentiality Agreement.

SECTION B:

Statement of Work

1. OVERVIEW

Contractor shall provide Chief Information Security Officer (“CISO”) advisory and 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. Contractor is expected to work directly with USAC staff and other contractors in order to satisfy the objectives of USAC’s Information Security Program.

USAC’s Information Security Program adheres to the Federal Information Security Management Act as amended by the Federal Information Security Modernization Act of 2014 (“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.

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

- Five (5) customer-facing business units which include: (1) Lifeline and the Affordable Connectivity Program, (2) E-rate and the Emergency Connectivity Fund, (3) Rural Health Care, (4) High Cost, and (5) Contributions that interact via web-based applications and application programming interfaces (“APIs”) with USF and the appropriated programs (the Affordable Connectivity Program and the Emergency Connectivity Fund), beneficiaries (schools, libraries, rural healthcare providers, low-income Lifeline subscribers), telecommunications service providers, and USF stakeholders. Each of these business units has no more than five (5) key systems. The majority of these systems are custom-built and on premise. More recent systems are managed in third-party vendor cloud environments.
- The business units are also supported by USAC internal systems including, but not limited to, the general support services (“GSS”), the enterprise database system (“EDS”), and the financial operations system, to include both the existing and the modernized financial systems.
- The business support units (HR, Internal Audit, OGC, and Information Technology) mostly have commercial off-the-shelf (“COTS”) based support systems that are configured to meet business unit requirements.

Contractor shall provide CISO advisory services to include:

1. Information Security Program management support
2. Cybersecurity Incident Response support
3. Information Security Awareness Training Support
4. Information Technology, Information Security, and Cybersecurity Audit Support

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 Offeror’s proposal 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 the awarded Contractor for any travel-related expenses.

3. CONTRACT TERM

The term of the Contract shall be for a base period of one year (the “Initial Term”) with three (3) one-year renewal options (each an “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 pursuant to Section C.31 or terminated sooner in accordance with the Contract. The Contract Term shall commence on the first day of the Contract period of performance (the “Effective Date”) as set forth in the Contract.

4. COMPANY PROFILE

USAC is a not-for-profit Delaware corporation operating 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; 200.324; 200.326-327 and App. II to C.F.R. Part 200 (collectively “Procurement Regulations”).

5. USAC PROGRAM MANAGER AND CONTRACTS ADMINISTRATOR

The Program Manager (“PM”) for the Contract will be a USAC employee in the Office of the Chief Information Security Officer (“OCISO”) designated by the CISO, the USAC point of contact for overseeing the performance of services. USAC’s Contracts Administrator (“CA”) for the Contract is TBD, the USAC point of contact for contractual matters (e.g. Contract administration, Contract modifications and other matters not related to performance).

6. WHERE THE WORK TAKES PLACE

- A.** All required services under the awarded Contract must be performed within the United States at either USAC’s headquarters at 700 12th Street NW, Suite 900, Washington, DC 20005 (“USAC Headquarters”), virtually, or at such other location as USAC may approve in its sole discretion. Presently, USAC has a hybrid work approach requiring Contractor Staff (as defined in Section C.1.G) to be in the USAC office at least 2 days per week.
- B.** Contract kick-off meeting may be held at USAC Headquarters or virtually. USAC will not reimburse Contractor for any travel related expenses for the kick-off meeting, status meetings, or other meetings.
- C.** Contractor shall schedule, coordinate, and hold a Contract kick-off meeting, no later than ten (10) workdays after any Contract award, at the location approved by USAC. The meeting will provide an introduction between Contractor Staff and USAC personnel who will be involved with the

awarded Contract. The meeting will provide the opportunity to discuss technical, management, and security issues, and review Contractor's proposed project timeline and reporting procedures. At a minimum, the attendees shall include Key Personnel (as described in Section C.1.N), Contractor Staff capable of obligating the Contractor, and USAC personnel.

- D. Services requiring work at USAC Headquarters will include appropriate workspace and appropriate access to USAC's computer network. **NOTE: To access USAC Information Technology ("IT") Systems, Contractor Staff must sign USAC's IT Security Rules of Behavior Form and complete mandatory IT security and privacy awareness online training. Contractor Staff may be required to complete role-based Privacy Act training if accessing USAC information systems designated as federal systems of records (i.e. National Verifier and National Lifeline Accountability Database – "NLAD").**
- E. Status update meetings and other meetings may be held virtually, except to the extent that USAC or Contractor requires in-person presence, and must be held in accordance with USAC and Contractor Continuity of Operations Plan ("COOP"). While present at USAC Headquarters for meetings or to perform the assigned activities, 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. Contractor may also be required to attend meetings at the FCC Offices located at 45 L Street NE, Washington, DC 20554.
- F. Upon written request by USAC, Contractor shall provide a COOP, including business continuity plans, disaster recovery plans, emergency operations plan and procedures, and associated plans and procedures in the event performance must be conducted virtually.
- G. Contractor shall comply with all guidance published by the Safer Federal Workforce Task Force for all Contractor Staff during the Contract Term (as defined in Section C.1.E of this RFP).

To provide adequate COVID-19 safeguards for USAC employees, Contractor shall ensure that all Contractor Staff that enter USAC premises will comply with USAC's COVID-19 Safety, Quarantine & Isolation Policy.

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

7. SCOPE OF SERVICES AND DELIVERABLES

Contractor shall provide the following Services (as defined in Section C.1.U):

- A. **Information Security Program Management Support:** Contractor shall provide senior subject matter expertise and trusted advisor support to the CISO and the overall OCISO. Contractor shall provide daily and strategic advisory support and assist in the day-to-day operation of the Information Security Program as well as support future strategic planning for short-, medium-, and long-term projects and initiatives by providing resources to perform the following:



- a. Strategic Advisory Support:** Contractor shall provide recommendations for strategic Information Security Program planning in accordance with CISO direction. Contractor shall review, develop, and consolidate strategic and operational plans, including requirements definition and mission planning. Long-term Information Security Program strategic plans shall be aligned to the USAC IT strategic goals, the IT strategic vision, and the IT strategic plan. To support this effort Contractor shall:
- i. Provide oversight and advisory services to assist the CISO with enterprise technical and programmatic issues as it relates to the USAC IT modernization efforts.
 - ii. Provide security compliance, cybersecurity, asset management, identity and access management, etc. recommendations to the appropriate stakeholders within the Information Security Program in support of comprehensive CISO operations.
 - iii. Serve as a senior analyst, in liaison with the major enterprise IT coordination function, such as IT project management office (“PMO”) and IT Product Management (“Product Management”) resources, to monitor ongoing business and systems activities and ensure the collaboration between the Information Security Program and these groups as well as to ensure new Information Security Program related activities are documented as demands, reviewed for their feasibility, and realistic schedules are identified for successful execution.
 - iv. Provide senior expertise in IT security planning across IT units in collaboration with the Information Security Program to ensure project plans developed for individual Information Security Program projects are realistic and achievable.
 - v. Develop a report on the state of IT from a cybersecurity perspective as well as a consolidated list of major IT risks to be delivered by the CISO to the “Chief Information Office (“CIO”) on an annual basis (“Annual Information Technology Risk Memo”) in collaboration with the IT Risk Management Program. In developing the Annual Information Technology Risk Memo, facilitate a final review with OCISO leadership and capture final approval by the CISO before submission to the CIO.
 - vi. Serve as the primary liaison with the FCC IT Security Team by:
 - 1) Monitoring, conducting, and/or contributing to all communications between the USAC Information Security Program and the FCC IT Security Team;
 - 2) Reviewing documentation and/or deliverables, as assigned, prior to being submitted to the FCC IT Security Team; and
 - 3) Facilitating and leading FCC bi-weekly IT security meetings including reviewing the agenda, leading preparation activities, reviewing meeting minutes, and conducting any follow ups needed post meeting.
 - vii. Develop the annual “Network Security Report” on behalf of USAC IT for delivery by the CISO to the FCC, which is a formal report to the FCC on the state of the USAC systems and infrastructure from a cybersecurity perspective. In developing the Network Security Report, facilitate a final review with IT Leadership and capture final approval by the CIO before submission to the FCC.



- viii. Develop and maintain a calendar of all major tasks, efforts, initiatives, and deliverables to be developed and/or delivered by the Information Security Program. This list of such items includes, but is not limited to:
 - 1) Annual Information Technology Risk Memo
 - 2) Network Security Report to the FCC
 - 3) Annual Cybersecurity Compliance Training
 - 4) Annual Role-based Cybersecurity Training
 - 5) IT Rules of Behavior Review and Recertification
- ix. Manage the structure, permissions, and access to CISO internal and external document repository.

b. Market Research and Studies: Market research shall be conducted by Contractor when required by the CISO. The market research shall involve exploring available COTS items, cloud-based functionality, and other commercial items via online resources.¹ Contractor shall assist in preparing the requirements for conducting market research, and, where appropriate, support in the preparation of draft requirements analyses, analyses of alternatives, and independent cost estimates. If market research requires communication with potential vendors, Contractor will coordinate with USAC's Procurement division before any action is taken. If there exists a conflict of interest in a requested market research request, this must be identified, documented, and presented to USAC immediately.

- i. Where appropriate, the market research shall meet the following objectives, at a minimum:
 - 1) Consider any laws, regulations, or government-wide policies or standards unique to the items under study,
 - 2) Gather and reveal information about distribution and support capabilities of suppliers, maintenance, and estimated costs, if available,
 - 3) Gather and reveal information about available sources, vendors, resellers and their capability,
 - 4) Gather and reveal information about mandatory sources for the product or services, and
 - 5) Gather and reveal information on hosting solutions that are compatible with the long-term strategy of the organization and that can be evaluated by IT.
- ii. When required by the CISO, Contractor shall conduct market research using a process (reviewed and approved by USAC Procurement) that provides information on the following, at a minimum:
 - 1) Existing and available products in the market,
 - 2) Potential capable sources,
 - 3) Competitive market forces,
 - 4) Generalized pricing information, if available online,

¹ USAC Procurement Department facilitates formal market research such as Requests for Information ("RFI") and handles communications with potential vendors



- 5) Varying levels of product performance and quality,
 - 6) Commercial practices, and
 - 7) Support capabilities.
- iii. Contractor shall evaluate alternative approaches in delivering fully capable system architectures, including leveraging existing systems where feasible. When required by the CISO, Contractor shall perform alternative system design studies that demonstrate potential for the following, at a minimum:
- 1) Reduced complexity,
 - 2) Lower cost,
 - 3) Quicker delivery schedules,
 - 4) Higher levels of performance or customer satisfaction, and
 - 5) Lower sustainment cost over the entire lifecycle of the system.
- c. Information Security Program Management Plan and Strategic Planning:** Contractor shall develop and maintain a plan which will codify the purpose and responsibilities of the Information Security Program (“Information Security Program Management Plan”) and provide updates at least annually. In doing so, Contractor shall:
- i. Develop a strategic and tactical Information Security Program Management Plan to include a method for tracking program maturity, performance, metrics, and improvement over time. This plan should:
 - 1) Use NIST and other applicable federal frameworks, resources, and guidance as benchmarks.
 - 2) Identify domains that require further development and provide recommendations for improvement plans; provide a maturity plan for each domain to strengthen USAC security posture.
 - ii. Develop a strategic five (5) year Information Security roadmap (“Security Roadmap”) and a tactical Information Security eighteen (18) month action plan (“Security 18-month Plan”) that provides recommendations on sequence and prioritization of major and minor cybersecurity initiatives to improve effectiveness across all security domains. The Security Roadmap should be updated annually, and the Security 18-month Plan should be updated quarterly.
 - iii. Collaborate with the IT PMO, IT Product Management, etc., resources to develop and implement project management oversight for the implementation of the eighteen (18) month action plan.
- d. Information Security Metrics:** Contractor shall formalize and standardize the reporting of information security metrics by performing the following:
- i. Develop a monthly metrics template designed to demonstrate key cybersecurity points of interest and risk to the executive level and provide updates at least annually.
 - ii. Collaborate across the OCISO to ensure that information security metrics are collected and consolidated to measure the Information Security Program’s



effectiveness. These metrics should be delivered at least monthly and will include, at a minimum, status and trends in each area:

- 1) IT System and Business Risks
 - 2) Active Vulnerabilities
 - 3) Assessment & Authorization
 - 4) Contingency Planning
 - 5) Incident Response
 - 6) Information Security Education, training, and awareness
- iii. Provide analysis and feedback at least annually to the CISO and OCISO leadership on the effectiveness and value of the metrics being collected and reported.

B. Cybersecurity Incident Response Support: Cybersecurity Incident Response is a key component of the Information Security Program, and Contractor shall contribute to the continual maturation and implementation of appropriate and substantial incident response by performing the following:

a. Collective Incident Response Plan: Contractor shall be responsible for developing and maintaining the “Collective Incident Response Plan”, which codifies USAC’s approach and steps for preparing for, responding to, and recovering from cybersecurity, privacy, fraud, operational, etc., incidents, and providing necessary updates on an annual basis. The Collective Incident Response Plan shall document USAC’s processes for preparing for and responding to cybersecurity, privacy, fraud, operational, etc., incidents. Contractor shall coordinate and collaborate with the USAC Privacy Officer, OGC, Director of Systems Operations, etc., in addressing the privacy, fraud, operational, etc., components of the Collective Incident Response Plan respectively. Contractor shall work closely with the CISO in documenting the cybersecurity components of the Collective Incident Response Plan.

b. Ransomware Response Plan: Contractor shall collaborate across the Information Security Program as well as the appropriate teams across USAC (i.e., OGC, EPI) and the FCC to document, finalize, and maintain the USAC “Ransomware Response Plan”, which will codify USAC’s approach and steps for preparing for, responding to, and recovering from a ransomware attack. Contractor shall review and provide updates to the Ransomware Response Plan at least annually.

c. Cybersecurity Incident Response Training Program:

- i. Develop and document a robust cybersecurity incident response training program, including training content, to assist with the education of all USAC employees and contractors. Monitor and take charge of ongoing maintenance of Cybersecurity Incident Response awareness and training needs for those with executive level and tactical information security incident response responsibilities (“Cybersecurity Incident Response Training Program”). Contractor shall ensure the Cybersecurity Incident Response Training Program is implemented and managed through collaboration with the USAC HR team. In addition, the Cybersecurity Incident Response Training Program must focus on, but not be limited to:



- 1) Functional-level knowledge of federal legislation and guidance applicable to incident response
 - 2) USAC Collective Incident Response Plan
 - 3) Integration of incident response processes with FCC, Department of Homeland Security (“DHS”), and other federal and law enforcement bodies
- ii. Develop and track metrics to assess the effectiveness of the Cybersecurity Incident Response Training Program to be delivered at least quarterly.

C. Information Security Awareness Training Support: In conjunction with the USAC CISO, Contractor shall be responsible for establishing and maintaining information-security awareness through a security awareness program by performing the following:

a. Cybersecurity Compliance Training Program:

- i. Develop a robust cybersecurity compliance training program, including training content, to assist with the education of all USAC employees and contractors, monitoring, and ongoing maintenance of general cybersecurity awareness and training needs (“Cybersecurity Compliance Training Program”). Contractor shall ensure that the Cybersecurity Compliance Training Program is implemented and managed through collaboration with USAC HR team. The Cybersecurity Compliance Training Program must initially focus on the following, and will be expanded as needed based on emergence of new directives or specific Cybersecurity training needs identified by the CISO:
 - 1) Basic information security concepts
 - 2) Cybersecurity threats
 - 3) Phishing
 - 4) Password Management
 - 5) Social Engineering
 - 6) Insider Threat
 - 7) Security incident/suspicious events reporting
- ii. Develop and track metrics to assess the effectiveness of the Cybersecurity Compliance Training Program to be delivered at least quarterly.

b. New Hire and Contractor Onboarding Cybersecurity Compliance Training Program:

- i. Develop a robust new hire and contractor onboarding cybersecurity compliance training program, including training content, to assist with the education of all USAC employees and contractors, monitoring, and ongoing maintenance of general cybersecurity awareness and training needs (“New Hire and Contractor Onboarding Cybersecurity Compliance Training Program”). Contractor shall ensure that the New Hire and Contractor Onboarding Cybersecurity Compliance Training Program is implemented and managed through collaboration with USAC HR team. The New Hire and Contractor Onboarding Cybersecurity Training Program must initially focus on the following, and will be expanded as needed based on emergence of new directives or specific cybersecurity training needs



identified by the CISO:

- 1) Basic information security concepts
 - 2) Cybersecurity threats
 - 3) Phishing
 - 4) Password Management
 - 5) Social Engineering
 - 6) Insider Threat
 - 7) Security incident/suspicious events reporting
- ii. Develop and track metrics to assess the effectiveness of the New Hire and Contractor Onboarding Cybersecurity Compliance Training Program to be delivered at least quarterly.

c. Role-based Cybersecurity Training Program:

- i. Develop, document and submit a robust role-based cybersecurity training program, including training content, to assist with the education of all USAC employees and contractors, monitoring, and ongoing maintenance of cybersecurity awareness and training needs for those with privileged and/or significant information security responsibilities (“Role-based Cybersecurity Training Program”). Contractor shall collaborate with the HR team to implement and manage the Role-based Cybersecurity Training Program. In addition, the Role-based Cybersecurity Training Program must initially focus on the following and will be expanded as needed based on emergence of new directives or specific cybersecurity role-based training needs identified by the CISO:
 - 1) Functional-level knowledge of information security federal legislation and guidance applicable to USAC
 - 2) USAC Information Security governance policies
 - 3) Cybersecurity best practices to cope with evolving cyber threats
 - 4) Fundamental requirements to establish a mature information security program
- ii. Develop and track metrics to assess the effectiveness of the Role-based Cybersecurity Training Program to be delivered at least quarterly.

d. IT Rules of Behavior: Review and update the IT Rules of Behavior on an annual basis with the following taken into account: industry best-practices, changes to information security and cybersecurity standards and policy, and feedback from within the Information Security Program, OGC, EPI, HR, and other teams across USAC. Coordinate with HR and EPI to ensure an up-to-date version is always posted in the appropriate, internally accessible location (i.e., USAC Intranet).

D. Information Technology, Information Security, and Cybersecurity Audit Support: At the direction of the CISO, Contractor shall be responsible for managing the strategic and day-to-day aspects of providing internal inspection and audit support by performing the following:



a. Annual FISMA Audit Support:

- i. Develop and maintain a “FISMA Audit Project Plan”, which will define both the actions to be taken in preparation for, during, and post annual FISMA Audit activities. The FISMA Audit Project Plan should also include an analysis of the prior year’s FISMA audit findings and the associated recommended remediation actions to be delivered annually. The FISMA audit is usually conducted between May and August, but this timeline is subject to change.
- ii. Provide an annual self-assessment against the current federal fiscal year Office of Inspector General (“OIG”) FISMA metrics (“FISMA Audit Self-Assessment”) with recommended actions for improving or maintaining current maturity status. In developing the FISMA Audit Self-Assessment, it is to be formally presented to OCISO leadership and IT Leadership on an annual basis before the commencement of each year’s annual FISMA Audit.
- iii. Provide audit support to the USAC CISO by overseeing and conducting pre-, during, and post-audit activities. These activities will include, at a minimum:
 - 1) Serve as a liaison between USAC and the FISMA auditors;
 - 2) Coordinate and track all audits requests, meetings, and deliverables;
 - 3) Provide weekly “FISMA Audit Weekly Status Reports” documenting, at a minimum, the status of all Provided by client artifacts (“PBC”), auditor meeting and observation session outcomes, any draft audit findings, and any suspected audit findings or issues;
 - 4) Draft and submit for USAC and FCC review and approval, corrective action plans (“CAPs”) for all FISMA findings to include prior year open findings, at the direction of the CISO and in coordination with USAC OGC, CIO, and EPI; and
 - 5) Draft and submit for USAC and FCC review and approval FISMA Audit Project Plan finding closure evidence once the appropriate action and documentation has been provided.

b. Internal and External AAD Audit Support:

- i. Provide audit support to the USAC CISO by overseeing and conducting pre-, during, and post-audit activities. These activities will include, at a minimum:
 - 1) Serve as a liaison between IT and the USAC Audit and Assurance Department (“AAD”) auditors;
 - 2) Coordinate and track all audit requests, meetings, and deliverables;
 - 3) Provide weekly “AAD Audit Weekly Status Reports” documenting, at a minimum, the status of all PBCs, auditor meeting and observation session outcomes, any draft audit findings, and any suspected audit findings or issues;
 - 4) Draft and submit for CIO review and approval, CAPs for all AAD Audit findings to include prior audit open findings, at the direction of the CISO and in coordination with EPI; and
 - 5) Draft and submit for CIO review and approval audit finding closure evidence once the appropriate action and documentation has been provided.



c. A-123 Audit Support:

- i. Provide audit support to the USAC CISO by overseeing and conducting pre-, during, and post-audit activities. These activities will include, at a minimum:
 - 1) Serve as a liaison between IT and the EPI;
 - 2) Coordinate and track all audit requests, meetings, and deliverables;
 - 3) Provide weekly “A-123 Exercise Weekly Status Reports” documenting, at a minimum, the status of all activities supporting the development of CAPs and/or entity level assessments (“ELA”) at the direction of the CISO; and
 - 4) Draft and submit for CIO review and approval, CAPs and/or ELAs at the direction of the CISO and in coordination with EPI. In developing the ELA, facilitate a final review with OCISO leadership and IT Leadership and capture final approval by the CISO and CIO before submission to EPI.

E. 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:

- i. Provide USAC with current versions of all system and user documentation;
- ii. Provide USAC all licensing and renewal information, asset management records, software documentation, and training materials;
- iii. Provide USAC with a current inventory of all USAC-owned assets used by Contractor along with full support in the reconciliation of this inventory;
- iv. 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
- v. 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.

F. Reporting: Contractor shall develop and deliver reports to communicate and showcase the accomplishments, deliverables from during the current month, and deliverables planned to be delivered in the subsequent month.

- a. Deliverable Schedule: Contractor shall develop a formal report that showcases a proposed comprehensive “Deliverable Schedule” incorporating all deliverables contained in this Section (Section B.7: Scope of Services and Deliverables) and when the Contractor proposes these to be delivered. The Deliverable Schedule should be presented for approval by USAC and reviewed at least monthly.
- b. Weekly Status Report: Contractor shall develop an informal report on a weekly basis that is a consolidated update of all activities and deliverables performed or delivered during the preceding week, as well as planned activities and deliverables for the subsequent week (as described in more detail in Section B.11.B.b. -- “Weekly Status Report”).

- c. Monthly Status Report: Contractor shall develop a formal report of all major/significant activities, accomplishments, and deliverables performed or delivered during the preceding month, as well as planned major/significant activities and deliverables for the subsequent month to be communicated to OCISO leadership (“Monthly Status Report”).

8. KEY PERSONNEL

USAC does not intend to dictate the composition of the ideal team to perform this Contract. Offeror shall provide consultant staffing for, at minimum, the labor category listed below. Offeror may also propose additional labor categories in its proposal submission. Any additional labor categories must include the experience and qualifications of the personnel to be assigned to that labor category. USAC requires that Key Personnel be assigned for the duration of the awarded Contract. Key Personnel may be replaced or removed subject to RFP requirements.

Security Program Consultant: The Security Program Consultant shall be responsible for managing the strategic and day-to-day aspects of the Information Security Program. The Security Program Consultant must have the following qualifications:

- Bachelor’s degree (master’s degree strongly preferred) and advanced relevant technical training and certifications. Eight (8) to ten (10) years of directly related work experience.
- Five (5) to seven (7) years of management experience.
- Three (3) to four (4) years of business leadership experience.
- Strong experience and knowledge in the following areas expected:
 - NIST
 - FISMA and FedRAMP
 - Audit Assessment Experience (internal and external)
 - Active Directory Systems
 - Network Security
 - Database Security
 - Operating Security
 - Application Security
 - System Security
 - Incident Response Management and Training
 - Enterprise IT Policy and Definitions
 - Forecasting/Budgeting

Preferred qualifications:

- CISSP Certified Information Systems Security Professional
- CISM Certified Information Security Manager
- SANS Certification
- PMP Certification

9. APPLICABLE DOCUMENTS

The work to be performed under the awarded Contract will assist USAC in better meeting legislative mandates and associated implementation guidance from the Office of Management and Budget (“OMB”),

NIST, DHS, FCC, and other federal agencies. Contractor must comply with, but not limited to, the following statutes, and acts:

1. Computer Security Act of 1987, PL 100-235
2. Federal Information Security Modernization Act of 2014 (FISMA)
3. Federal Cybersecurity Workforce Assessment Act of 2015
4. OMB Memorandum M-14-03: Enhancing the Security of Federal Information and Information Systems
5. OMB Circular A-130 and Appendix III, Security of Federal Automated Information Resources
6. OMB Circular A-123, Management's Responsibility for Internal Control
7. Presidential Decision Directives
8. Executive Orders (such as 14028)
9. NIST Cybersecurity Framework
10. USAC, current policies for Information Systems Security and Privacy
11. E-Government Act of 2002
12. Clinger-Cohen Act of 1996
13. Computer Fraud and Abuse Act of 1986
14. NIST Special Publications – 800 Series
15. NIST Federal Information Processing Standards
16. The Privacy Act of 1974
17. Section 508 of the Rehabilitation Act of 1973

10. 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	Annually	Annual Information Technology Risk Memo	(Section B. 7.A.a.v.) Develop and submit a report on the state of IT from a cybersecurity perspective as well as a consolidated list of major IT risks to be delivered by the CISO to the CIO on an annual basis.
02	As Requested	Communications and Deliverables to FCC	(Section B.7.A.a.vi.1-2.) Serve as the primary liaison with the FCC IT Security Team by: monitoring, conducting, and/or contributing to all communications between the USAC Information Security Program and the FCC IT Security Team; and reviewing documentation and/or deliverables, as assigned, prior to being submitted to the FCC IT Security Team.
03	Bi-weekly	FCC IT Security Meeting Preparation and Facilitation	(Section B.7.A.a.vi.3.) Facilitate and lead the FCC bi-weekly IT security meetings by reviewing the agenda, leading preparation activities, reviewing meeting minutes, and conducting any follow ups needed post meeting.

#	Frequency	Deliverable	Description
04	Annually	Network Security Report	(Section B.7.A.a.vii.) Develop and submit the annual “Network Security Report” on behalf of USAC IT for delivery by the CISO to the FCC.
05	Quarterly	Information Security Program Calendar Updates	(Section B.7.A.a.viii.) Develop and maintain for review a calendar of all major tasks, efforts, initiatives, and deliverables to be developed and/or delivered by the Information Security Program. This list of such items includes, but is not limited to: <ol style="list-style-type: none"> 1. Annual Information Technology Risk Memo 2. Network Security Report to the FCC 3. Annual Cybersecurity Compliance Training 4. Annual Role-based Cybersecurity Training 5. IT Rules of Behavior Review and Recertification
06	Ongoing	CISO Document Repositories	(Section B.7.A.a.ix.) Manage the structure, permissions, and access to CISO internal and external document repository.
07	As Requested	Market Research and Studies	(Section B.7.A.b.) Deliver formal and informal market research and studies as requested by the CISO and/or OCISO.
08	Annually	Information Security Program Management Plan and Updates	(Section B.7.A.c.i.) Contractor shall develop, maintain and submit a plan which will codify the purpose and responsibilities of the Information Security Program and provide updates at least annually.
09	Annually	Security Roadmap	(Section B.7.A.c.ii.) Develop and submit a strategic five (5) year Information Security roadmap that provides recommendations on sequence and prioritization of major and minor cybersecurity initiatives to improve effectiveness across all security domains.
10	Quarterly	Security 18-Month Plan	(Section B.7.A.c.ii.) Develop and submit a tactical Information Security 18-month Plan that provides recommendations on sequence and prioritization of major and minor cybersecurity initiatives to improve effectiveness across all security domains.
11	Annually	Monthly Metrics Template	(Section B.7.A.d.i.) Contractor shall formalize and standardize the collection reporting of Information Security metrics by developing and submitting a monthly metrics template designed to demonstrate key cybersecurity points of interest and risk to the executive level, review and update at least annually.
12	Monthly	Monthly Metrics Report	(Section B.7.A.d.ii.) Collaborate across the OCISO to ensure information security metrics are collected and consolidated to measure the Information Security Program’s effectiveness.

#	Frequency	Deliverable	Description
13	Annually	Analysis and Feedback of Metrics Template	(Section B.7.A.d.iii.) Provide analysis and feedback at least annually to the CISO and OCISO leadership on the effectiveness and value of the metrics being collected and reported.
14	Annually	Collective Incident Response Plan	(Section B.7.B.a.) The Collective Incident Response Plan shall document USAC's processes for preparing for and responding to cybersecurity, privacy, fraud, operational, etc., incidents. Contractor shall review and provide updates to the Collective Incident Response Plan at least annually or more frequently at the request of the CISO.
15	Annually	Ransomware Response Plan	(Section B.7.B.b.) Contractor shall collaborate across the Information Security Program as well as the appropriate teams across USAC (i.e., OGC, EPI) and the FCC to document, finalize and deliver the USAC Ransomware Response Plan. Contractor shall review and provide updates to the Ransomware Response Plan annually or more frequently at the request of the CISO.
16	Annually	Cybersecurity Incident Response Training Program	(Section B.7.B.c.i.) Develop and document a robust Cybersecurity Incident Response Training Program, including training content, to assist with the education of all USAC employees and contractors. Monitor and take charge of ongoing maintenance of Cybersecurity Incident Response awareness needs for those with executive level and tactical information security incident response responsibilities. Contractor shall review and provide updates to the Cybersecurity Incident Response Training Program annually.
17	Quarterly	Cybersecurity Incident Response Training Program Metrics	(Section B.7.B.c.ii.) Develop and track metrics to assess the effectiveness of the Cybersecurity Incident Response Training Program.
18	Annually	Cybersecurity Compliance Training Program	(Section B.7.C.a.i.) Develop and document a robust cybersecurity compliance training program, including training content, to assist with the education of all USAC employees and contractors, monitoring, and ongoing maintenance of general cybersecurity awareness and training needs. Contractor shall review and provide updates to the Cybersecurity Compliance Training Program annually.
19	Quarterly	Cybersecurity Compliance Training Program Metrics	(Section B.7.C.a.ii.) Develop and track metrics to assess the effectiveness of the Cybersecurity Compliance Training Program.

#	Frequency	Deliverable	Description
20	Annually	New Hire and Contractor Onboarding Cybersecurity Training Program	(Section B.7.C.b.i.) Develop, document and submit a robust New Hire and Contractor Onboarding Cybersecurity Compliance Training Program, including training content, to assist with the education of all USAC employees and contractors, monitoring, and ongoing maintenance of general cybersecurity awareness needs. Contractor shall review and provide updates to the New Hire and Contractor Onboarding Cybersecurity Training Program annually.
21	Quarterly	New Hire and Contractor Onboarding Cybersecurity Training Program Metrics	(Section B.7.C.b.ii.) Develop and track metrics to assess the effectiveness of the New Hire and Contractor Onboarding Cybersecurity Compliance Training Program.
22	Annually	Role-based Cybersecurity Training Program	(Section B.7.C.c.i.) Develop, document and submit a robust Role-based Cybersecurity Training Program, including training content, to assist with the education of all USAC employees and contractors, monitoring, and ongoing maintenance of general cybersecurity awareness needs. Contractor shall review and provide updates to the Role-based Cybersecurity Training Program annually.
23	Quarterly	Role-based Cybersecurity Training Program Metrics	(Section B.7.C.c.ii.) Develop and track metrics to assess the effectiveness of the Role-based Cybersecurity Training Program.
24	Annually	IT Rules of Behavior Review and Update	(Section B.7.C.d.) Review and update the IT Rules of Behavior on an annual basis with the following taken into account: industry best-practices, changes to information security and cybersecurity standards and policy, and feedback from within the Information Security Program, OGC, EPI, HR, and other teams across USAC.
25	Annually	FISMA Audit Project Plan	(Section B.7.D.a.i.) Develop, maintain and submit a FISMA Audit Project Plan including an analysis of the prior year's FISMA audit findings and associated recommended remediation actions to be delivered annually prior to the annual FISMA audit.
26	Annually	FISMA Audit Self-Assessment	(Section B.7.D.a.ii.) Provide a self-assessment against the current federal fiscal year OIG FISMA metrics with recommended actions for improving or maintaining current maturity status.

#	Frequency	Deliverable	Description
27	Weekly (during Audit)	FISMA Audit Weekly Status Reports	(Section B.7.D.a.iii.1-3.) Provide weekly audit status reports documenting, at a minimum, the status of all PBCs, auditor meeting and observation session outcomes, any draft audit findings, and any suspected audit findings or issues
28	Annually	FISMA Audit Correction Action Plans	(Section B.7.D.a.iii.4.) Draft and submit for USAC and FCC approval CAPs for all FISMA findings to include prior year open findings, at the direction of the CISO and in coordination with USAC OGC, CIO, and EPI.
29	As-Needed	FISMA Audit Finding Closure Evidence Submission	(Section B.7.D.a.iii.5.) Draft and submit for USAC and FCC review and approval FISMA audit finding closure evidence once the appropriate action and documentation has been provided.
30	Weekly (during Audit)	AAD Audit Weekly Status Reports	(Section B.7.D.b.i.1-3.) Provide weekly audit status reports documenting, at a minimum, the status of all PBCs, auditor meeting and observation session outcomes, any draft audit findings, and any suspected audit findings or issues
31	As-Needed	AAD Audit Correction Action Plans	(Section B.7.D.b.i.4.) Draft and submit for CIO approval CAPs for all AAD audit findings to include prior open findings, at the direction of the CISO and in coordination with EPI.
32	As-Needed	Audit Finding Closure Evidence Submission	(Section B.7.D.b.i.5.) Draft and submit for CIO review and approval Audit finding closure evidence once the appropriate action and documentation has been provided.
33	Weekly (during Exercise)	A-123 Weekly Status Reports	(Section B.7.D.c.3.) Provide weekly exercise status reports documenting, at a minimum, the status of all activities supporting the development of CAPs and/or ELAs at the direction of the CISO.
34	Annually	A-123 ELA	(Section B.7.D.c.4.) Draft and submit for CIO review and approval, CAPs and/or ELA at the direction of the CISO and in coordination with EPI.
35	One-time	Transition In Plan (within five (5) business days of contract award)	(Section B.7.E.) Develop a 60-day plan for onboarding all resources and providing support for USAC teams and deliverables.
36	One-time	Transition Out Plan [No later than sixty (60) days before end of contract period of performance]	(Section B.7.E.) Develop a 60-day plan for onboarding resources and providing support for USAC teams for the knowledge transfer of all deliverables and responsibilities.

#	Frequency	Deliverable	Description
37	One-time (with monthly update)	Deliverable Schedule	(Section B.7.F.a.) Develop a proposed comprehensive deliverable schedule incorporating all deliverables contained in this section and when the Contractor proposes these to be delivered; proposed deliverable schedule to be presented for approval by USAC and reviewed at least monthly. <i>Note: all deliverables need to be accompanied by a Deliverable Acceptance Form (“DAF”) in order to be formally accepted by USAC.</i>
38	Weekly	Weekly Status Report	(Section B.7.F.b.) Provide an informal weekly consolidated update of all activities and deliverables performed or delivered during the preceding week as well as planned activities and deliverables for the subsequent week. <i>Note: a consolidation of all previously mentioned weekly status reports will be acceptable. Additionally, this deliverable includes reporting on all activities performed or requested in accordance with all subsections of Section B.7 not directly associated with a deliverable listed in this table (i.e., oversight and advisory services, recommendations, demand and project schedule generation, etc.).</i>
39	Monthly	Monthly Status Report	(Section B.7.F.c.) Provide a formal report of major/significant activities, accomplishments, and deliverables performed or delivered during the preceding month as well as planned major/significant activities and deliverables for the subsequent month to be communicated to USAC leadership.

11. MEETINGS

A. 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.

B. Weekly Status Meetings

- a. Key Personnel must schedule and participate in weekly status meetings. Physical travel to USAC's office for attendance and participation will be required, as needed; otherwise, virtual attendance and participation is required.
- b. Contractor shall prepare the Weekly 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 at noon (12:00 PM ET) during weeks in which the meeting is scheduled for Monday, or when no status meeting is scheduled. The Weekly Status Report shall be used as the basis of the status meeting discussion.

C. 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 must 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.

D. Accessibility

- a. 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. “Code” means the United States Bankruptcy Code.
- C. “Confidential Information” is defined in Section 16 of these USAC Standard Terms and Conditions.
- D. “Contract” means these USAC Terms and Conditions (including the attached USAC Standard Terms and Conditions Privacy and Security Addendum), 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.
- E. “Contract Term” means the Initial Term of these USAC Standard Terms and Conditions and any executed Optional Renewal Terms.
- F. “Contractor” means the Offeror (as defined elsewhere in the Contract) whose proposal was selected for award of the Contract.
- G. “Contractor Staff” 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 Staff” also includes the entity that employs Contractor’s employees, subcontractors, consultants, and agents in all cases except where the context clearly references only individuals.
- H. “Courts” means the district and, if applicable, federal courts located in the District of Columbia.
- I. “Deliverables” means the goods, items, products, and materials that are to be prepared by Contractor and delivered to USAC as described in the Contract.
- J. “Derivative Works” means any and all modifications or enhancements to, or any new work based on, in whole or in part, any USAC Data, Confidential Information, Software, or Deliverable regardless of whether such modifications, enhancements or new work is defined as a “derivative work” in the Copyright Act of 1976.
- K. “Discloser” means a party to this Contract that discloses Confidential Information to the Recipient.



- L. “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.
- M. “Initial Term” means the original duration of these USAC Standard Terms and Conditions as described in Section 2 of these USAC Standard Terms and Conditions.
- N. “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.
- O. “Optional Renewal Term” means an additional one year period that can extend the duration of these USAC Standard Terms and Conditions, and that can be exercised at USAC’s sole discretion as described in Section 2 of these USAC Standard Terms and Conditions.
- P. “Privacy and Security Addendum” means the part of this document that includes most of the language regarding Contractor’s obligations around protecting USAC Data.
- Q. “Procurement Regulations” mean the following provisions of the Code of Federal Regulations: 2 C.F.R. §§ 200.318-321, 200-324, 200.326-327 and App. II to C.F.R. Part 200.
- R. “Recipient” means a party to this Contract that receives Confidential Information from a Discloser.
- S. “SAM” means the System for Award Management or suspension or debarment status of proposed subcontractors that can be found at <https://www.sam.gov>.
- T. “SAN” means the Supplier Actionable Notification, which is a method of paying USAC invoices.
- U. “Services” means the services, tasks, functions, and responsibilities described in the Contract.
- V. “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.
- W. “Solicitation” means the request for Services described in the Contract.
- X. “Sub-Recipient” means a partner, joint venturer, director, employee, agent, or subcontractor of a Recipient to whom a Recipient must disclose Confidential Information.
- Y. “UCSP” means the USAC Coupa Supplier Portal, which is a method of paying USAC invoices.
- Z. “USAC” means Universal Service Administrative Company.

- AA. “USAC Data” 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 Data is Confidential Information and subject to all requirements in Section 16 of these USAC Standard Terms and Conditions.
- BB. “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).
- CC. “USAC Standard Terms and Conditions” means this document that provides the legal terms that govern this Contract.
- DD. “USF” means the Universal Service Fund.

2. TERM

The Initial Term is the period of time from the Effective Date (as defined in the cover sheet to this Contract) of the Contract to _____. After the conclusion of the Initial Term, USAC will have the right to extend the Contract Term by exercising up to _____ () 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 Standard Terms and Conditions, 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 Standard Terms and Conditions and any other document made part of the Contract, the USAC Standard Terms and Conditions shall govern. 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 Standard 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 UCSP method or via the SAN method. The UCSP method will require Contractor to register and create an account for the UCSP. An invitation link to the UCSP 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 Standard 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.

Contractor will promptly credit to USAC any payment made to which Contractor is not entitled under these USAC Standard Terms and Conditions and refund to USAC any such payment for which there are not sufficient fees against which to credit the overpayment.

Under no circumstance will USAC be liable to pay Contractor any fees not invoiced within ninety (90) days after Contractor was first permitted to invoice USAC as described in Section 6 of these USAC Standard Terms and Conditions.

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, delegatee, 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, delegatee, 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 Staff 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, as appropriate, to USAC and deliver to USAC, or as directed by USAC, all USAC Data, Confidential Information, 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 demands 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 Staff in connection with this Contract; and (c) any claims or demands of any nature whatsoever to the extent caused by Contractor's breach of any confidentiality, security, or privacy obligations set forth in these USAC Standard Terms and Conditions by Contractor or Contractor Staff; (d) Contractor's unauthorized use of USAC Software, USAC IT Systems, or USAC Data; (e) any breach of applicable law as described in Section 27 of these USAC Standard Terms and Conditions by Contractor or Contractor Staff; or (f) the negligent, reckless, illegal, or intentional acts or omissions of Contractor or Contractor Staff in connection with the performance of the Services.

16. CONFIDENTIAL INFORMATION

- A. *Confidential Information.* Confidential Information includes, but is not limited to, USAC 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, or 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 [defined in the USAC Standard Terms and Conditions Privacy and Security Addendum.]; 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 Staff, 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 Privacy Officer 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 Staff 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 USAC 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 DATA

- A. *Return or Destruction of USAC Data.* Except as provided in Section 17.B of these USAC Standard 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 Data, including all copies thereof, in the possession or under the control of Contractor or Contractor Staff. If USAC directs that Contractor destroy any USAC Data, then, at USAC's request, Contractor shall provide USAC with an executed certificate in writing stating that all such USAC Data was destroyed.



- B. *Acknowledgement of Data Inclusion in Federal System of Record.* Contractor acknowledges and agrees that certain USAC Data may be included in a federal system of record and is subject to record retention schedules set forth by the National Archives and Record Administration and to USAC's records retention policy. Upon expiration or termination of the Contract, information subject to the National Archives and Record Administration's schedules or to 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 Data to USAC.
- C. *No Withholding of USAC Data.* Contractor shall not withhold any USAC Data 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 Data 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 Data, 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. ["NIST" is defined in the USAC Standard Terms and Conditions Privacy and Security Addendum.]
- F. *No Other Use.* USAC Data is provided to Contractor solely for the purpose of rendering the Services, and USAC Data 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 Data, modified, decompiled, reverse engineered, or commercially exploited by or on behalf of Contractor, Contractor Staff, or any third party.

18. PROPRIETARY RIGHTS

Contractor agrees that all USAC Data, Software, Deliverables, and all Derivative Works thereof are USAC property and shall be deemed USAC Data 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 a waiver from Contractor Staff 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 USAC Data, Software, Deliverables, 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 USAC Data, Software, Deliverables, or 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 USAC, incorporate any USAC Data, Software, Deliverable, or Derivative Work thereof delivered under the Contract not first produced in the performance of the Contract unless Contractor: (a) identifies the USAC Data, Software, Deliverable, or 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 USAC Data, Software, Deliverable, or Derivative Work thereof in any way.

19. RESPONSIBILITY FOR CONTRACTOR STAFF

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

Contractor shall conduct background checks on Contractor Staff and provide evidence of the background checks to USAC upon request.

20. 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.

21. 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.

22. 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.

23. 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 as USAC, 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 of this Contract. 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.

24. 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.

25. 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 term valid and enforceable.

26. 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.

27. 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, and 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; and the laws and guidelines named in the USAC Standard Terms and Conditions Privacy and Security Addendum.

28. 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 of 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 USAC Data, Software, Deliverable, or any Derivative Work thereof.

29. 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.

30. INDEPENDENT CONTRACTOR

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

31. 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.

32. NOTICES

All notices, consents, approvals 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.

33. 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 Data, confidentiality obligations, proprietary rights, and indemnification obligations shall survive the expiration or termination of the Contract.

34. 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 continues to take 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.

35. 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.

36. 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 of 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 Contractor 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 36.D of these USAC Standard 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 36.B. of these USAC Standard 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 36.B. of these USAC Standard Terms and Conditions, Contractor shall 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 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:
 - 1. 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);
 - 2. If the service is not associated with maintenance, the product service code of the service being provided; and
 - 3. 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 supporting evidence for all certifications.

37. PROHIBITION ON A BYTEDANCE COVERED APPLICATION

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

1. “*Covered Application*” means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.
2. “*Information Technology*” means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by USAC, if the equipment is used by USAC directly or is used by Contractor under this Contract with USAC that requires the use—
 - (a) Of that equipment; or
 - (b) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

The definition of “*Information Technology*” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

The definition of “*Information Technology*” does not include any equipment acquired by a Contractor incidental to this Contract.

- B. Prohibition. Contractor is prohibited from having or using a Covered Application on any Information Technology owned or managed by USAC, or on any Information Technology used or provided by Contractor under this Contract, including equipment provided by Contractor Staff.
- C. Subcontracts. Contractor shall insert the substance of this clause, including this subsection C, in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

38. ADDED SERVICES

USAC may at any time submit a request that Contractor perform any Added Services. Before Contractor performs any 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.

39. ADEQUATE COVID-19 SAFETY PROTOCOLS

Contractor shall comply with all guidance published by the Safer Federal Workforce Task Force for all Contractor Staff during the Contract Term.

To provide adequate COVID-19 safeguards for USAC employees, Contractor shall ensure that all Contractor Staff that enter USAC premises will comply with USAC's COVID-19 Safety, Quarantine & Isolation Policy.

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

40. PRIVACY AND SECURITY ADDENDUM

Contractor must comply with the privacy and security requirements and obligations found in the USAC Standard Terms and Conditions Privacy and Security Addendum.

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.

USAC STANDARD TERMS AND CONDITIONS

PRIVACY AND SECURITY ADDENDUM

This is the USAC Standard Terms and Conditions Privacy and Security Addendum to, and hereby incorporates, the USAC Standard Terms and Conditions between Universal Service Administrative Company (“USAC”) and [REDACTED]. (“Contractor”), dated as of **INSERT DATE** (the “USAC Standard Terms and Conditions”). Capitalized terms used but not defined herein shall have the meanings ascribed to such terms in the Contract.

1. DEFINITIONS

“Authority to Operate” or “ATO”	The official management decision given by a USAC official or officials to authorize operation of an information system and to explicitly accept the risk to USAC operations (including mission, functions, image, or reputation), USAC assets, individuals, and other organizations based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
“Contractor IT”	Any information technology device, software, hardware, equipment, system, and/or any IaaS, PaaS, or SaaS provided by a CSP that is owned or managed by the Contractor, its agents, or subcontractors.
“Cloud Protocols”	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.
“Cloud Service Offering”	A service from a cloud service provider. FedRAMP categorizes Cloud Service Offerings as one of the following: IaaS, PaaS, or SaaS.
“Cloud Service Provider” or “CSP”	A provider of IT infrastructure, product, or SaaS to be acquired by a user of IT services.
“COTS”	Commercial off-the-shelf Software, which is Software, hardware, and information technology products that (1) already exist, (2) are available from commercial sources, (3) are ready-made, and (4) are available for purchase by the general public.
“Cybersecurity/Data Breach”	A successful incident in which sensitive, confidential, or otherwise protected system/data has been accessed and/or disclosed in an unauthorized fashion. For example, a brute force attack against a protected system, attempting to guess multiple usernames and passwords, is a Cybersecurity Incident, but cannot be defined as a Cybersecurity/Data Breach unless the attacker succeeded in guessing a password.



	<p>If a Cybersecurity Incident grants the attacker access to protected systems, it may qualify as a Cybersecurity/Data Breach. If the attacker obtained access to USAC Data, it is a Cybersecurity/Data Breach.</p> <p>Not every Cybersecurity Incident is a Cybersecurity/Data Breach, Privacy Incident, or a Privacy Breach. Most Cybersecurity Incidents do not result in an actual Cybersecurity/Data Breach.</p> <p>Examples of Cybersecurity/Data Breaches may include, but are not limited to:</p> <ul style="list-style-type: none"> • Bringing down the USAC.org website (for example, through a Denial of Service (DoS) Attack. • Employee causes ransomware to be installed and encrypts computer or entire network (Phishing Attack, DoS Attack) • Attacker obtains USAC Data through unauthorized access. • Unencrypted USAC Data being disseminated through peer-to-peer file sharing service.
<p>“Cybersecurity Incident”</p>	<p>An event that attempts to or successfully compromises the integrity, confidentiality, and/or availability of an information asset or USAC Data. A Cybersecurity Incident could be either intentional or accidental in nature. Cybersecurity incidents hereafter may be referred to as a “Cyber Incident” or “Incident”.</p>
<p>“Data at Rest”</p>	<p>State of data while it is on the device that stores it, or data that has reached a destination and is not being accessed or used. This term is primarily used in the context of data encryption. It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory waiting to be read or updated. It does not include data in use while it is being processed, accessed, or read where it must be decrypted to be used.</p>
<p>“Data in Transit”</p>	<p>Data transmitted via email, web, collaborative work applications, instant messaging, or any type of private or public communication channel. This term is primarily used in the context of data encryption. It includes all data moving between systems or devices on networks. It does not include data in use while it is being processed, accessed, or read where it must be decrypted to be used.</p>
<p>“Data Leakage”</p>	<p>The inadvertent exposure of data beyond its controlled environment or intended usage, such as a lost or stolen laptop, an employee storing files using an Internet storage application, or an employee saving files on a USB drive to take home.</p>

“Data Loss”	The exposure of proprietary, sensitive, or classified information through either Data Theft or Data Leakage. This includes the intentional or unintentional destruction of information, caused by people and or processes from within or outside of an organization. In a Cybersecurity/Data Breach or Privacy Breach the data is compromised, but Data Loss further describes damage to the integrity, completeness, or control of the data.
“Data Safeguards”	Protections that safeguard USAC Data against destruction, loss, damage, corruption, alteration, loss of integrity, commingling, or unauthorized access or Processing.
“Data Security Laws”	FISMA, 44 U.S.C. § 3541, et seq., the Privacy Act as amended (as may be applicable), and NIST SP 800-53 Rev 5. PII protections 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 NIST SP 800-61 Rev 2 (or most current version), and FIPS 140-3. Any federally mandated information security and privacy requirements not described herein.
“Data Theft”	The deliberate or intentional act of stealing information such that controlled data is intentionally stolen or exposed, such as in cases of espionage or employee disgruntlement.
“Event”	An exception to the normal operation of IT infrastructure, systems, services, or privacy. Not all Events become a Cybersecurity Incident or Privacy Incident. Cybersecurity Incidents and Privacy Incidents are Events which can represent a threat, an attack, or a breach.
“Exfiltration”	The unauthorized transfer of information from USAC IT Systems.
“FedRAMP-Authorized,” or “FedRAMP Authorization”	A term used to designate a Cloud Service Offering from a CSP that satisfies the security assessment, authorization, and continuous monitoring requirements of the Federal Risk and Authorization Management Program (“FedRAMP”), a US government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies; see FedRAMP.gov.
“FIPS”	Federal Information Processing Standards. FIPS are standards and guidelines for computer systems that are developed by NIST in accordance with FISMA and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular requirement.
“FISMA”	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.
“IaaS”	Infrastructure as a service.
“Malicious Code” or	Any software, hardware, firmware, program, routine, protocol, script, code,

<p>“Malware”</p>	<p>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) designed to (i) disrupt, disable, deactivate, interfere with, or otherwise compromise USAC IT Systems, or (ii) access, modify, disclose, transmit, or delete PII, Confidential Information, or USAC Data; or (b) either inadvertently or upon the occurrence of a certain event, compromises the confidentiality, integrity, privacy, security, or availability of PII, Confidential Information, USAC Data, or USAC IT Systems. Examples of Malicious Code include, but are not limited to, viruses, worms, bugs, ransomware, spyware, bots, backdoors, devices, root kits, and Trojan Horses.</p> <p>For purposes of this definition, “root kits” are a set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means.</p>
<p>“Malicious Cyber Activity”</p>	<p>Any activity, other than those activities authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information systems, communications systems, networks, or physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.</p>
<p>“Multifactor Authentication”</p>	<p>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, but are not limited to: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); and/or (iii) something you are (e.g., biometric).</p>
<p>“NIST” and “NIST SP”</p>	<p>NIST means the National Institute of Standards and Technology, part of the U.S. Department of Commerce. NIST SP means a special publication published by NIST.</p>
<p>“OMB”</p>	<p>Office of Management and Budget.</p>
<p>“PaaS”</p>	<p>Platform as a service.</p>
<p>“Personally Identifiable Information” or “PII”</p>	<p>Personally Identifiable Information (PII) is defined as information 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.</p> <p>Examples of PII include name, address, telephone number, date and place of birth, mother’s maiden name, biometric records, social security number, etc.</p>
<p>“PIN”</p>	<p>Personal Identification Number</p>

“Privacy Breach”	A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to PII. When PII is involved in a Cybersecurity/Data Breach it then becomes a Privacy Breach.
“Privacy Incident”	An unauthorized use or disclosure of confidential, sensitive, or regulated data, like USAC Data, PII, or confidential commercial information. For example, an unauthorized user gains access to a system containing PII and exfiltrates the PII.
“Process” or “Processing”	Any operation or set of operations that is performed using USAC Data, whether or not by automatic means, including, but not limited to, collection, retention, logging, generation, transformation, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, destruction, transfer, or disposal.
“Risk Management Framework” or “RMF”	A seven (7) step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of FISMA.
“SaaS”	Software as a service.

2. SECURITY PROVISIONS

- 2.1 Data Security Laws Compliance. Contractor shall comply with the Data Security Laws. For any Contractor IT using a Cloud Service Offering that accesses, stores, or otherwise processes USAC Data, and/or PII, Contractor shall provide documentation and proof of FedRAMP Authorization 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 or the complete package of documents for any Cloud Service Offering with agency accreditation.
- 2.2 Contractor Compliance Generally. 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 this Privacy and Security Addendum or the USAC Standard Terms and Conditions.
- 2.3 Contractor Duties Prior to Delivering Services. Prior to delivering the Services or enabling data-sharing or interoperability of any kind with USAC IT Systems, Contractor shall: (i) demonstrate Contractor system is compliant with FISMA and NIST SP 800-53 Rev. 5 and has received an Authority to Operate by the Contractor’s authorizing official after following the steps laid out in the NIST risk management framework by providing evidence thereof; (ii) 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; (iii) complete any security questionnaires, IT rules of behavior, certifications, assessments, or workforce training reasonably requested by USAC in a timely manner; and (iv) receive prior written authorization from USAC to access USAC IT Systems 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, their establishment shall be at Contractor's sole cost and expense. Under no circumstances shall USAC's written authorization to access USAC IT Systems serve as a representation or warranty by USAC that such access is secure or as a waiver of any rights in this Privacy and Security Addendum or the USAC Standard Terms and Conditions. Failure to satisfy the conditions set forth in subsections (i) – (iv) herein to USAC's reasonable satisfaction shall be considered a material breach of the USAC Standard Terms and Conditions by Contractor.

- 2.4 Contractor Security Policies. Throughout the Contract Term, Contractor shall establish and maintain appropriate internal policies and procedures regarding: (i) the security of the Services and Contractor IT systems; and (ii) the permitted use, disclosure, access to, and security of PII, USAC Data, 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 IT and the access information (e.g. name, username, password, access rights) of all Contract Staff, to immediately remove access for persons no longer authorized, and to inform USAC immediately if Contractor suspects, or reasonably should suspect, there is unauthorized access to USAC Data or the USAC IT System. Contractor shall require Contract Staff to use Multifactor Authentication. Contractor agrees to require all who have access to USAC IT Systems through Contractor to maintain the confidential nature of the Confidential Information, and to not use or access USAC IT Systems except for the benefit of USAC.
- 2.5 Compliance Plan. In providing the Services, Contractor's Data Safeguards shall be no less rigorous than the most protective of: (a) the requirements of applicable Law; (b) the specific standards set forth in this Article; and (c) the applicable USAC standards relating to data security. The parties shall execute an interconnection security agreement prior to any required establishment of direct interconnection between Contractor IT and USAC IT Systems.
- 2.6 PII. Contractor shall ensure that: (i) PII shall be protected in accordance with all laws and USAC requirements, including, without limitation, relevant: (a) OMB Memorandum M-17-12; (b) guidance from the NIST including without limitation the most current revision of NIST SP 800-53 Rev. 5; and (c) FCC requirements or the most current replacement of the above; (ii) to the extent that cloud-based Services are to be employed by Contractor and interact with USAC Data, Contractor shall provide documentation and proof of FedRAMP-Authorization to demonstrate compliance, and such Services shall be certified by FedRAMP for use at a moderate risk by the time the cloud-based Services are implemented (USAC reserves the right to inspect the Authority to Operate or the complete package of documents for those with agency accreditation); and (iii) all Cybersecurity Incidents or Privacy Incidents resulting in any interruption to system services, including the disclosure of PII, shall be tracked in accordance with NIST SP 800-53 Rev. 5, NIST SP 800-61, and OMB Memorandum M-17-12.
- 2.7 Contractor Responsible for Contract Staff. Contractor shall ensure that all Contract Staff will be bound by the same or substantially similar restrictions on collection, use, disclosure, and retention of PII, Confidential Information, USAC Data, and USAC Software. Contractor shall be

responsible for any breach of data security or privacy-related obligations by any Contract Staff and shall fully indemnify USAC for any damages incurred as a result of such breach. Contractor will be required to provide annual information security and privacy awareness training to all Contract Staff that will be working under the USAC Standard Terms and Conditions prior to having access to USAC Data or to USAC IT Systems. All Contract Staff will also be required to sign USAC's IT rules of behavior as well as confidentiality and non-disclosure agreements as required by third parties and USAC.

- 2.8 Vendor Insider Threat Program. Vendor will submit Vendor's insider threat program (as required by NIST 800-53 Rev. 5 (see controls PM-12, IR-4(6), IR-4(7), and SI-4(12)) to USAC's Chief Privacy Officer and USAC's Chief Information Security Officer within ninety (90) days of the Effective Date of the Contract. If USAC has any questions regarding Vendor's insider threat program, Vendor will make Contract Staff knowledgeable of Vendor's insider threat program available to USAC upon USAC's request.
- 2.9 Encryption and Secure Storage. PII must be encrypted at all times in accordance with FIPS 140-3 standards. This encryption requirement includes both Data at Rest and Data in Transit. 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 the USAC Terms and Conditions and this Privacy and Security Addendum.
- 2.10 Further Requirements. Contractor's applications, processes, and systems used in providing the Services shall be approved by USAC's IT security team and shall comply with FISMA, NIST, and OMB requirements. Contractor shall demonstrate Authority to Operate for any system that will temporarily or permanently house USAC Data, in compliance with NIST standards, and will provide all relevant documentation as defined in the NIST RMF lifecycle therein. Contractor further agrees to provide any assistance requested by USAC to enable Contractor or USAC to comply with FISMA requirements, including, without limitation, at Contractor's expense, providing USAC with periodic documentation and reports demonstrating FISMA compliance, system accreditation, and correction of any weakness or deficiency (as defined by FISMA) attributable to Contractor that would prevent Contractor or USAC from complying with FISMA. Contractor shall be responsible at its sole expense to remediate any FISMA noncompliance of its systems or the Services. No less than annually, Contractor shall write, review, and update an assessment of its compliance with all applicable federal mandates and other industry-accepted standards as set forth in this Article to ensure adherence thereto. Contractor will also perform any and all activities needed to ensure continued compliance with all federal mandates and other industry-accepted standards as set forth in this Article.
- 2.11 Contractor Assumption of the Risk. Contractor agrees that access to PII, USAC Data, Confidential Information, and USAC IT Systems is at USAC's sole discretion, and that Contractor's access to such systems 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 IT Systems by Contractor and Contract Staff, including any data-sharing or interoperability between USAC and Contractor, shall be for the sole purpose of providing the Services. Contractor agrees that: (i) USAC IT Systems are owned solely by USAC; (ii) USAC will monitor the use of USAC IT Systems; (iii) neither

Contractor nor Contract Staff have any expectation of privacy with regard to USAC IT Systems; and (iv) all information appearing on USAC IT Systems (except for information publicly disclosed by USAC) will be considered Confidential Information. Contractor will not use USAC IT Systems except as expressly authorized by USAC. USAC requires that Contract Staff use a USAC.org email address when providing Services. Contractor agrees that its use of, and access to, USAC IT Systems is completely at its own risk.

2.12 Contractor's Obligation for Subcontractors. Contractor agrees to ensure that any subcontractor that accesses, receives, maintains, or transmits PII, USAC Data, Confidential Information, or USAC IT Systems agrees to the same restrictions and conditions that apply to Contractor under this Privacy and Security Addendum and the USAC Standard Terms and Conditions.

2.13 Performance Within 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 Contract Staff; and (b) storage and/or processing of data and/or other virtual Services (such as cloud storage, remote data processing, *etc.*).

2.14 Cybersecurity Incidents and Privacy Incidents

2.14.1 Contractor Must Notify USAC of Cybersecurity Incidents and Privacy Incidents. Contractor shall examine any Event that is an exception to the normal operation of IT infrastructure, systems, services, or privacy in order to identify if the Event represents a threat, an attack, or a breach. Any Event identified as a Cybersecurity Incident or Privacy Incident requires that USAC be notified at incident@USAC.org and Privacy@USAC.org within one (1) hour of becoming aware of an actual or suspected Cybersecurity Incident or Privacy Incident.

2.14.2 Notification Requirements. Contractor's notice to USAC shall include the following: (i) a description of the Cybersecurity Incident or Privacy Incident, including the date of the Cybersecurity Incident or Privacy Incident and the date of discovery by Contractor, if known; (ii) a description of the type(s) of Malicious Code, PII, USAC Data, Confidential Information, or USAC IT Systems involved in the Cybersecurity Incident or Privacy Incident, if any; (iii) if applicable and 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 Cybersecurity Incident or Privacy Incident; (iv) a brief description of what Contractor is doing to investigate the Cybersecurity Incident or Privacy Incident and mitigate the harm to USAC; (v) any steps Contractor recommends USAC should take to protect itself from potential harm resulting from the Cybersecurity Incident or Privacy Incident; (vi) the name, phone number, and e-mail address of Contractor's representative responsible for responding to the Cybersecurity Incident or Privacy Incident; 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, USAC Data, Confidential Information, or the USAC IT Systems. Contractor will regularly supplement its notice(s) with additional information as it becomes available.

2.14.3 Contractor Responsibilities Prior-to and After Cybersecurity Incident or Privacy Incident.

Contractor, working with USAC, shall use its best efforts to mitigate and eliminate the effects of the Cybersecurity Incident or Privacy Incident on USAC and, if the Cybersecurity Incident or Privacy Incident 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 Cybersecurity Incident or Privacy Incident (including participating in any needed forensic investigation and law enforcement investigations) 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 Cybersecurity Incident or Privacy Incident and coordinate with Contract Staff 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 USAC Standard Terms and Conditions, if the Cybersecurity Incident or Privacy Incident is due to the negligence or misconduct of Contractor or Contract Staff, 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 breach mitigations, under this Section as a result of the Cybersecurity Incident or Privacy Incident. Failure to strictly abide by the USAC Standard Terms and Conditions and this Privacy and Security Addendum shall be considered a material breach of the USAC Standard Terms and Conditions for which USAC shall have the right to immediately terminate for cause.

2.15 Backups. Contractor shall automatically make backups of all USAC Data files found in Contractor's information technology systems. Such backup shall be in a format that is readily accessible and usable by USAC.

2.16 Security Audit. USAC or its designated USAC auditor 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 Contractor locations. Contractor is responsible for remediation of any identified weakness or findings of noncompliance.

2.17 Security and Privacy Assessments. Contractor shall provide support for assessments of FISMA compliance on an annual basis. Security and privacy assessments may include, but are not limited to, third party assessments to achieve FISMA ATO or to maintain continuous monitoring and ongoing authorization of a Contractor IT system in compliance with the RMF and controls described in NIST SP 800-53 Rev 5. The assessment process may also include security penetration testing to identify additional vulnerabilities through ethical hacking and compliance challenging techniques. Assessments shall include but shall not be limited to: (a) Contractor's documented and demonstrated internal controls and procedures related to the Services; (b) cooperation with USAC IT security or privacy staff in connection with testing the effectiveness of such controls and procedures; (c) making at least quarterly representations to USAC regarding any significant changes to such controls and procedures; (d) documenting and tracking all identified material weaknesses or deficiencies reported by an assessment, penetration test, Cybersecurity Incident,

Privacy Incident, or any other deficiency that would prevent USAC from complying with law, using a Plan of Action and Milestones (“POA&M”) process; and (e) cooperating with USAC auditors in connection with the issuance of the reports described in Section 2.20 of this Privacy and Security Addendum. Contractor shall promptly remediate any weakness identified in any assessment, in no event later than recommended or demanded by the assessors.

2.18 Notification and Assistance. Contractor will cooperate with USAC in any litigation and investigation deemed necessary by USAC to protect USAC Data, other USAC Confidential Information, and/or PII. Each party will bear the costs it incurs as a result of compliance with this Section.

2.19 Vulnerability Management. Contractor shall address vulnerabilities in accordance with NIST vulnerability management controls including, but not limited to, addressing vulnerabilities in the applicable timeframes set forth in such policies. Contractor shall provide a monthly vulnerability report and a risk mitigation plan to address any identified vulnerabilities. Critical and high vulnerabilities, as defined in NIST management controls, shall be reported to the USAC Chief Information Officer and Chief Information Security Officer, and Contractor shall remedy such vulnerabilities as soon as possible. Contractor shall provide USAC a POA&M to address such vulnerabilities promptly and shall prioritize remediation based on the risks implicated by such vulnerabilities.

2.20 Additional Requirements for Services in Contractor IT

- If Contractor becomes aware that the Services in Contractor IT will lose or has lost its respective FedRAMP Authorization, Contractor shall notify USAC within twenty-four (24) hours, shall discontinue use of such Services, and shall initiate activities to replace the Services that have lost FedRAMP Authorization. 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 Authorization 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 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 10 business days) to any new or supplemental information security questions that 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 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) calendar days of the Effective Date.
- Contractor shall maintain administrative, technical, physical, and procedural information security controls as demonstrated in Service Organization Controls (“SOC”) 2 Type II reports. Contractor shall maintain these controls and notify USAC of any changes to its compliance. Contractor shall provide USAC with its most current SOC 2 Type II report within ten (10) calendar days of the Effective Date
- On an annual basis, upon written request, Contractor will provide USAC with the most current versions of following:
 - Contractor security policies referenced in Section 2.4 of this Privacy and Security Addendum;
 - Standard Information Gathering (SIG) Lite documentation;
 - SOC 2 Type II report;
 - System ATO(s) or evidence of effective Information Security Continuous Monitoring (ISCM) in compliance with FISMA and NIST SP 800-53 Rev. 5;
 - ISO 27001 certifications.

3. TECHNOLOGY CONSIDERATIONS

- 3.1 **Deployment in Cloud.** Contractor shall ensure that SaaS, PaaS, or IaaS Cloud Service Offerings, or COTS, deployed in Contractor IT cloud or on any USAC-acquired CSP infrastructure, satisfies the following requirements:
- 3.1.1 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 FedRAMP Authorized CSP identity and access management product used by USAC.
 - 3.1.2 Any USAC Data stored in a database that is a component of a CSP SaaS, PaaS, or IaaS, or a COTS, must be readily available to USAC in industry standard formats that enable USAC to access, copy, or transfer USAC Data as required.
 - 3.1.3 Any SaaS, PaaS, or IaaS Software must maintain the Authority to Operate and FedRAMP Authorization for the Contract Term.
- 3.2 **Custom Software.** Contractor shall ensure that any custom Software developed and/or deployed for USAC, whether on USAC premise, on a USAC or Contractor cloud, or on a hybrid infrastructure:

- 3.2.1 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.
- 3.2.2 Reuses available USAC technology services (including microservices and application programming interfaces) 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.
- 3.2.3 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. Details of USAC's technical stack and service architecture will be provided as appropriate.

4. **MALICIOUS CODE AND MALICIOUS CYBER ACTIVITIES**

USAC may provide Contractor access to one or more 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 Contract Staff should have any expectation of privacy with regard to use of USAC IT Systems, and that all information appearing on 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 USAC IT Systems except as expressly authorized by USAC in this Privacy Security Addendum and the USAC Standard Terms and Conditions. Contractor agrees to maintain strict control of all Contract Staff usernames, passwords, and access lists for USAC IT Systems, 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 USAC IT Systems through Contractor to maintain the confidential nature of all Confidential Information, and to not use USAC IT Systems except for the benefit of USAC. Contractor agrees that it will use 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 IT, 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 Contractor introduced Malicious Code into any USAC IT System, or 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. If the Malicious Code or Malicious Cyber Activity causes a loss of operational efficiency or loss of data, Contractor will 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 Contract Staff 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.

If Malicious Code is introduced into USAC IT Systems, and/or Contractor or Contract Staff has engaged in Malicious Cyber Activity involving USAC IT Systems, it shall be considered a Cybersecurity Incident or Privacy Incident. If Contractor becomes aware that Malicious Code has been introduced into USAC IT Systems, or Contractor or Contract Staff has engaged in Malicious Cyber Activity, Contractor will notify USAC within one (1) hour of becoming aware.

SECTION D: Attachments

Attachment List:

- Attachment 1: Bid Sheet
- Attachment 2: Reserved
- Attachment 3: Confidentiality Agreement
- Attachment 4: Deliverable Acceptance Form

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 of all Sections of this RFP, including any attachments listed in Section D. Offeror’s submission of a proposal constitutes Offeror’s agreement to the RFP and its precedence over any other terms, requirements, or conditions proposed by Offeror.

Offeror’s proposal may identify deviations from, or revisions, exceptions or additional terms (collectively “exceptions”) to the RFP, 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 RFP 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 that are included in Offeror’s proposal. After selection of the awardee, USAC will not consider or negotiate any exceptions to the RFP.

B. PERIOD FOR ACCEPTANCE OF OFFERS

Offeror agrees to hold the pricing 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. 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 August 15, 2023** (“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-23-053, of this RFP.

C. PROPOSAL SCHEDULE

Key activities and target completion dates are set forth below. USAC may change these dates at its sole discretion and convenience, without liability.

DATE	EVENT
July 12, 2023	RFP Released
July 20, 2023	Questions due to USAC by 11:00 AM ET at rfp@usac.org
July 26, 2023	Q&A Released To Potential Offerors
August 15, 2023	Proposal Due to USAC by 11:00 AM ET at rfp@usac.org
October 2023	Anticipated Award Date

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. SUBMISSION OF QUESTIONS

USAC will only accept written questions regarding the RFP. All questions must be emailed to rfp@usac.org no later than **July 20, 2023, 11:00 AM ET**. USAC plans to post all questions and responses under this procurement on our website by **July 26, 2023, 5:00 PM ET**.

E. 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. 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

Offeror's proposal shall clearly and conspicuously identify information contained in the proposal that the Offeror contends is Confidential Information. *See* Section C.16.

4. PROPOSAL FORMAT

Proposals shall be presented in four separate volumes:

1. Volume 1 – Corporate Information
2. Volume 2 – Technical Capability
3. Volume 3 – Past Performance
4. Volume 4 – Price

5. PROPOSAL COVER PAGE

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

- The name of Offeror's organization,
- Offeror's contact name,
- Offeror's contact information (address, telephone number, email address, website address),
- Offeror's Unique Entity ID 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 representative.

6. PROPOSAL CONTENT

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

A. Corporate Information (Volume 1)

1. A cover page, as outlined above.
2. *Executive Summary*. This section shall summarize all key features of the proposal, affiliated individuals, or firms that Offeror proposes to assist in this engagement. Pricing information shall not appear in the Executive Summary.
3. *Confidentiality and Information Security*. Offeror must explain in detail how they will establish and maintain safeguards to protect the confidentiality and integrity of USAC Confidential Information in their possession as required by the solicitation.
4. *Conflict of Interest*. Offeror must provide a statement regarding any known conflicts of interest. USAC is the appointed neutral administrator of the federal USF. USAC is governed by a Board of Directors comprised of various stakeholders in the universal service programs and is prohibited from advocating positions on universal service policy matters. Because of USAC's unique role as neutral administrator, it is essential that any contractor providing assistance to USAC in administering the USF maintain the same neutrality, both in fact and in appearance.
 - 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 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 Offeror (or proposed subcontractor) and any USF Stakeholder; (2) 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 Offeror; (4) an USAC or FCC employee receives any type of compensation from 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 Offeror or any proposed subcontractor; and (7) any ownership or control interest in Offeror or any proposed subcontractor that is held by an FCC or USAC employee. Offerors must also identify any participation by Offeror, or any proposed subcontractor(s) or personnel associated with Offeror, in any of the universal service programs. The requirement in this Section E.6.A.4.b applies at all times until Contract execution.

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

B. Technical Capability (Volume 2)

This volume must include:

1. A cover page, as outlined above.
2. **Technical Approach:** An in-depth discussion of Offeror's technical approach to providing the services outlined in Section B, along with a clear statement of whether or not Offeror's performance of the Contract will comply with all requirements stated in this RFP, including the USAC Terms and Conditions set forth in Section C. Offerors must submit a detailed response to this RFP. Any deviations from, or exceptions to, the requirements in this RFP, including the USAC Terms or Conditions set forth in Section C, must be clearly identified in a separate Attachment to the proposal.

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

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 Offeror's expertise in performing engagements of this type as illustrated by Offeror's description of how it proposes to perform the requirements set forth in this RFP.



3. **Capabilities:** Describe Offeror's capabilities for performing the Services under the awarded 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.
4. **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.

C. Past Performance Information (Volume 3)

This volume must include:

1. A cover page, as outlined above.
2. Description of Offeror's recent 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.
3. A list of up to three (3) current or recently completed contracts for services 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 Offeror's proposal. Although

USAC will follow-up with the contacts, Offeror, not USAC, is responsible for ensuring that the questionnaire is completed and returned by the specified date in USAC's transmittal. If USAC is unable to reach or obtain a reference for the project, USAC may not consider the contract in an evaluation of past performance.

D. Price Proposal (Volume 4)

This volume must include:

1. A cover page, as outlined above.
2. Completed pricing information in **Attachment 1 – Bid Sheet**.
 - a. The proposed price must be *fully loaded* and must include wages, overhead, general and administrative expenses, taxes, and profit.

E. Presentation and Page Limitations

1. Proposal Presentation
 - a. Proposals must be prepared using Times New Roman font. All text except for diagrams, tables, and charts must be presented in 12-point font. Diagrams, tables, and charts may be presented in a smaller font if needed to fit the page. The reduced font size may not be smaller than 9 point.
 - b. The content of each diagram, table, Gantt chart, and chart must accurately depict the same information included in the text, serving as the visual representation of the written content in the proposal.
 - c. Any diagram, table, Gantt chart or chart must be readable when printed. These documents may be included as attachments to the proposal using landscape orientation to enhance presentation if needed.
 - d. All diagrams, tables, Gantt charts, and charts must be incorporated into the proposal using the native program from which it was created to eliminate distortion of text by inserting images and pictures.
 - e. The font color used to label column headings must be bolded and a contrasting color from the background color to clearly display headings.
 - f. Each volume of the proposal should be submitted in PDF format as a separate attachment to a single email to rfp@usac.org. **Attachment 1 – Bid Sheet** may be submitted as a separate attachment in Excel format as an addition to Volume 4.
 - g. The signed RFP cover page and signed Confidentiality Agreement may be submitted in PDF format as separate attachments and will not count towards the page limits for volumes 1–4 of the Offeror's proposal.
2. Page Limitation

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

 - a. Volume 1 – Corporate Information; may not exceed four (4) pages.

- b. Volume 2 – Technical; may not exceed twelve (12) pages; however excluding **Attachment A** (Resumes).
- c. Volume 3 – Past performance information; may not exceed five (5) pages.
- d. Volume 4 – Price; may not exceed four (4) pages.

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

7. EVALUATION

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 shall be used to evaluate 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. Capabilities
 - c. Key Personnel
2. **Experience and Past Performance:** Experience and past performance information will be evaluated to assess the risks associated with Offeror’s performance of this effort, considering the relevance, how recent the project is (no older than three (3) years from the date of the solicitation), and quality of Offeror’s past performance on past or current contracts for the same or similar services. Offeror’s past performance will be evaluated based on Offeror’s discussion of its past performance for similar efforts, information obtained from past performance references (including detailed references for 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 Offeror’s proposal that are not identified as references).
3. **Price Evaluation:** USAC will evaluate price based on the firm fixed price listed in **Attachment 1 – Bid Sheet**. 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. In addition to considering the total prices of 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.

8. 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.

9. RESPONSIBILITY DETERMINATION

USAC will only award contracts to responsible Offerors. 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. Offeror has sufficient resources to perform the Services described in the RFP;
2. Offeror has a satisfactory record of performance, integrity, and business ethics;
3. 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. Offeror has the facilities, and technical and personnel resources required to perform the contract; and
5. Offeror is not excluded from government contracting, as listed on the excluded parties list in <https://www.sam.gov>.



Attachment 1

Bid Sheet

[Separate Excel Attachment]

Attachment 3

USAC Confidentiality Agreement

This USAC Confidentiality Agreement (the “Confidentiality Agreement”) is entered into by and between the Universal Service Administrative Company (“USAC”), the disclosing party, and _____, located at _____ (the “Receiving Party”) for the purpose of preventing the unauthorized disclosure of Confidential Information as defined below. The parties agree to enter into a confidential relationship with respect to the disclosure of certain proprietary and confidential information (“Confidential Information”).

1. The Receiving Party recognizes and acknowledges that as a potential contractor, subcontractor, consultant, agent, or other representative thereof (collectively, a “Contractor”) for the Universal Service Administrative Company (“USAC”), it may have access to Confidential Information, as that term is defined in Appendix A to this Confidentiality Agreement.
2. The Receiving Party acknowledges and agrees that it will treat any Confidential Information in the manner set forth in this Confidentiality Agreement. The Receiving Party acknowledges and agrees that this obligation applies to the treatment of all Confidential Information to which it obtains access while performing services or applying to perform services on behalf of USAC, regardless of the form of the Confidential Information or the manner in which it obtains access to the Confidential Information. The Receiving Party acknowledges and agrees that its obligations with respect to Confidential Information apply to oral and written communications, drafts and final documents, information obtained directly or indirectly if the Receiving Party obtained the information as a result of its relationship with USAC.
3. The Receiving Party acknowledges and agrees that its obligation to treat Confidential Information in the manner set forth in this Confidentiality Agreement will continue even if it is no longer a Contractor.
4. The Receiving Party acknowledges and agrees that it will not use Confidential Information for any purpose other than a legitimate business purpose of USAC.
5. The Receiving Party acknowledges and agrees that, except as provided in paragraphs 6 and 7 herein or as authorized by the USAC Chief Executive Officer or the USAC General Counsel, or in either one’s absence, a respective designee, the Receiving Party will not disclose Confidential Information to any other person or entity.
6. The Receiving Party acknowledges and agrees that this Confidentiality Agreement shall not apply to requests for Confidential Information made by an employee of the Federal Communications Commission (“Commission”), except that the Receiving Party may not disclose Personally Identifiable Information (as that term is defined in Appendix A to this Confidentiality Agreement) without the express advance written approval of the USAC Chief Executive Officer or the USAC General Counsel, or in either one’s absence, a respective designee.
7. The Receiving Party acknowledges and agrees that, subject to the notice requirement in paragraph

8 below, this Confidentiality Agreement shall not prevent disclosure of Confidential Information in response to an official request from the Comptroller General of the United States, the Government Accountability Office, or the United States Congress or a Committee or Subcommittee thereof, except that the Receiving Party may not disclose Personally Identifiable Information without the express advance written approval of the USAC Chief Executive Officer or the USAC General Counsel, or in either one's absence, a respective designee.

8. The Receiving Party acknowledges and agrees that if it receives a subpoena or any other request or demand for Confidential Information, the Receiving Party will take all reasonable and appropriate steps such that the request is submitted within one business day of receipt, and prior to any disclosure of such information or records, to the USAC General Counsel, or in the USAC General Counsel's absence, a respective designee.
9. The Receiving Party acknowledges and agrees that if it knows or has a reasonable basis for believing that any USAC staff person or other person or entity is using or disclosing Confidential Information in violation of this Confidentiality Agreement, it will immediately so notify the USAC General Counsel.
10. The Receiving Party acknowledges and agrees that if it intentionally or unintentionally discloses any Confidential Information in violation of this Confidentiality Agreement, it will immediately so notify the USAC General Counsel.
11. The Receiving Party acknowledges and agrees that if it is uncertain or has questions about its obligations under this Confidentiality Agreement, the Receiving Party will immediately seek advice from the USAC General Counsel.
12. The Receiving Party acknowledges and agrees that any violation of this Confidentiality Agreement may subject it to disciplinary action, including suspension or termination of its relationship with USAC, and civil and criminal liability.
13. The Receiving Party acknowledges and agrees that signing this Confidentiality Agreement is a condition of applying to perform services and/or performing services as a Contractor for USAC. The Receiving Party acknowledges and agrees that USAC may modify this Confidentiality Agreement and require it to execute the modified version.
14. The Receiving Party acknowledges and agrees that upon completion or termination of its relationship as a Contractor for USAC, the Receiving Party will return to the USAC General Counsel or other person designated by them, any Confidential Information in its possession.
15. The Receiving Party acknowledges and agrees that this Confidentiality Agreement is binding upon it as of the date of the signature of the Receiving Party, that any modification to this Confidentiality Agreement is binding on the Receiving Party as of the date that it signs such modified version, and that its obligations under the Confidentiality Agreement, including any modifications, continue through and beyond the termination of its position as a Contractor and for as long as it has in its possession, access to, or knowledge of Confidential Information. The Receiving Party further acknowledges and agrees that USAC may, in its sole discretion, modify Appendix A and such

modification(s) shall be effective and enforceable against the Receiving Party following written notice to the Receiving Party, which may be by any reasonable method, including but not limited to hand delivery, mail, courier service, email, or facsimile, and that its signature or agreement is not required for the modification to Appendix A to be effective and binding on the Receiving Party.

16. If any provision of this Confidentiality Agreement is determined by a court of competent jurisdiction to be invalid or unenforceable, that provision shall be deemed stricken and the remainder of the Confidentiality Agreement shall continue in full force and effect as if it had been executed without the invalid provision.

17. This Confidentiality Agreement shall be governed by and construed in accordance with the Laws of Washington D.C., without giving effect to the principles thereof relating to the conflicts of laws. The parties agree that the state and federal courts located in Washington D.C. shall have exclusive jurisdiction with respect to any dispute, controversy, or claim arising out of or relating to this Confidentiality Agreement.

Acknowledged and agreed:

By (signature) _____

Name (print) _____

Date _____

CONFIDENTIALITY AGREEMENT – APPENDIX A

Personally Identifiable Information is defined as information 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.

Confidential Information is defined as:

1. Information, data, material, or communications in any form or format, whether tangible or intangible, including notes, analyses, data, compilations, studies, or interpretations (collectively referred to hereafter as “information”) and any data, material or communications in any form or format, whether tangible or intangible, that contains, reflects, or is derived from or based upon any information or is related to internal USAC management matters, including but not limited to USAC program integrity procedures, if disclosure is reasonably likely to interfere with or prejudice the performance of the internal USAC management functions.

2. Information related to the development of statements of work or evaluation criteria for USAC or Commission procurements, contractor bids or proposals, evaluation of bidders or offerors, selection of contractors, or the negotiation of contracts.
3. Information that is excluded by applicable statute or regulation from disclosure, provided that such statute (a) requires that the information be withheld from the public in such a manner as to leave no discretion on the issue, or (b) establishes particular criteria for withholding or refers to particular types of information to be withheld. Such information includes copyrighted or trademarked information.
4. Information containing trade secrets or commercial, financial or technical information that (a) identifies company-specific (i.e., non-aggregated) proprietary business information about a Universal Service Fund (USF) contributor (or a potential contributor) or its parent, subsidiary, or affiliate, and (b) has not previously been made publicly available.
5. Information concerning USAC relationships with financial institutions, including but not limited to, account locations, identifiers, balances, transaction activity and other account information and any advice or guidance received from such institutions.
6. Information regarding or submitted in connection with an audit or investigation of a USF contributor, potential USF contributor, USF beneficiary, applicant for USF support, or USAC Staff Person.
7. Information to which USAC, the Commission, or any other government agency might assert a claim of privilege or confidentiality, including but not limited to attorney-client communications, information that constitutes work product or reflects USAC, Commission or other government agency decision-making processes, including law enforcement investigations and program compliance matters. Such information includes but is not limited to internal USAC information, information exchanged between USAC and the Commission or another government agency, and information exchanged between two or more government agencies in any form, including but not limited to letters, memoranda, draft settlement documents, and working papers of USAC, the Commission, other government agencies, and their respective staff.
8. Information that was submitted with a corresponding written request for confidential treatment, protection, or nondisclosure, including, but not limited to, submissions marked “proprietary,” “privileged,” “not for public disclosure,” or “market sensitive information,” unless and until such request is denied.
9. Information developed in security investigations. Such information is the property of the investigative agency and may not be made available for public inspection without the consent of the investigative agency.

Attachment 4: Deliverable Acceptance Form

Purpose: The purpose of this “Deliverable Acceptance Form” is to provide verification that deliverable(s) have been reviewed and accepted by USAC.

PROJECT IDENTIFICATION		
Date of Deliverable Submitted	Project Name	Contract Number
Contractor Project Manager		USAC Project Manager

DESCRIPTION OF DELIVERABLE

Signatures indicates the following:

- USAC acknowledges that the deliverable(s) contained herein have been reviewed and USAC has verified that the deliverable(s) meet the SOW scope.
- Contractor acknowledges that there are no unfulfilled obligations remaining for the deliverable(s) contained on this Deliverable Acceptance Form as of the below date.

ACCEPTED BY	
USAC Project Manager	
Contractor Project Manager	