# USAC Solicitation for IT Security Operations Center Services – 2nd Revision

## SOLICITATION INFORMATION:

| | |
|---|---|
| Method of Solicitation: | Request for Proposal ("RFP") |
| Contract Period of Performance: | One Year, plus Two (2) Option Years |
| Contract Effective Date: | TBD 2023 |
| Solicitation Number: | RFP IT-23-064 |
| Solicitation Issue Date: | April 6, 2023 |
| Questions Due Date: | April 17, 2023 |
| Proposal Due Date: | May ~~9~~17, 2023 |

## CONTRACT TO BE ISSUED BY:

Universal Service Administrative Company ("USAC")
700 12th Street, NW, Suite 900
Washington, D.C. 20005

## CONTACT INFORMATION:

| USAC CONTACT INFORMATION | OFFEROR CONTACT INFORMATION |
|---|---|
| Anthony Smith<br>Procurement Specialist<br>Phone: 202-916-3486<br>Email: Anthony.Smith@usac.org | (complete)<br>Name: _____<br>POC: _____<br>POC Title: _____<br>POC Phone: _____<br>POC Email: _____<br>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, General Counsel, Information Systems, Audit and Assurance, Enterprise Program Management, and Human Resources.

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.

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

## 2. PURPOSE

The purpose of this RFP is to acquire professional services for 24/7/365 managed services and monitoring of USAC's Splunk Cloud and Splunk enterprise security environment. This includes alert triage and tier 1 incident response.

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

# SECTION B:

# Statement of Work

## 1. PROJECT OVERVIEW

The USAC Information Security Team is looking for a vendor to provide 24/7/365 proactive and reactive Security Operations Center ("SOC") services to support its existing internal staff. USAC is seeking an external SOC to assist in reviewing daily alerts, track security incidents, and analyze user reported issues in a detailed and timely manner. Other activities will include providing maturation and support of USAC's Splunk environment, providing artifacts for audits and assessments, and support the implementation and execution of NIST 800-53 Rev. 5 security controls and continuous monitoring activities. In addition, Contractor will conduct threat hunting, incident response, tabletop exercises, and contribute to incident response planning.

USAC has implemented a suite of well-known security tools across the organization to detect malware, protect against phishing and spam, log events, and monitor the environment. Contractor shall use, and shall have experience with, the security tools implemented in the USAC environment and Contractor shall perform analysis on alerts and logs coming from the USAC IT Systems (as defined in Section C.1.BBB). Information on the security tools that are being used is provided in Attachment 2. Additionally, Contractor will be required to make recommendations on fine tuning alerts and other configurations to streamline detection and analysis of events.

Contractor must have a proven track record of embedding resources into an already existing and maturing team of similar size and scope to the USAC Security Operations team. Any Key Personnel (as defined in Section C.1.FF) assigned to the awarded Contract should be at the highest skill level and will remain working on the Services (as defined in Section C.1.VV) for the duration of the awarded Contract. This includes designating appropriate staffing levels for increased log generation and threat hunting activities.

## 2. 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").

## 3. PLACE OF PERFORMANCE

**A.** All required Contract 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, D.C. 20005 ("USAC Headquarters"), virtually, or such other location as USAC may approve in its sole discretion. Presently, USAC has a hybrid work approach requiring contractors that work in USAC's office to be in the USAC office at least 2 days per week.

**B.** A Contract kick-off meeting may be held at USAC Headquarters or virtually. USAC will not reimburse Contractor for any travel related expenses for kick-off, status, and other meetings.

**C.** Contractor shall schedule, coordinate and hold a Contract kick-off meeting, no later than five (5) workdays after award, at the location approved by USAC. The meeting will provide an introduction between Contractor Personnel (as defined in Section C.1.J) and USAC personnel who will be involved with the awarded Contract. The meeting will provide the opportunity to discuss technical, management, and security issues, review Contractor's proposed project timeline, and reporting procedures. At a minimum, the attendees shall include Contractor Key Personnel (as described in Section 11.F of this RFP), Contractor Personnel 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 IT Systems, Contractor must sign USAC's IT Security Rules of Behavior Form and complete mandatory IT Security and Privacy Awareness Online Training. Contractor may be required to complete Role-Based Privacy Act Training if accessing USAC information systems designated as federal system of records (i.e., National Verifier and National Lifeline Accountability Database (or "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 in accordance with USAC and Contractor Continuity of Operations Plan ("COOP"). While attending USAC Headquarters for meetings or to conduct audits, Contractor Personnel will be considered as visitors. All visitors are required to complete USAC's 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, D.C. 20554.

**F.** Contractor shall comply with all guidance published by the Safer Federal Workforce Task Force for all Contractor Personnel during the Contract Term (as defined in Section C of this RFP).

To provide adequate COVID-19 safeguards for USAC employees, Contractor shall ensure that all Contractor Personnel that enter USAC premises will comply with USAC's COVID-19 Vaccination Validation & Testing 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.

**G.** 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.

## 4. ABBREVIATIONS

The following abbreviations are used in this RFP and the awarded Contract:

| Abbreviation | Description |
|---|---|
| CLIN | Contract Line Item Number |
| FFP | Firm-Fixed-Price |
| T&M | Time and Materials |
| NTE | Not to Exceed |
| NLT | No Later Than |

## 5. CONTRACT TYPE

The awarded Contract will be a blended FFP and T&M single award Contract with a NTE ceiling price stated in **Attachment 1** – Bid Sheet.

## 6. CONTRACT TERM

The initial term of the awarded Contract shall be for twelve (12) months ("Initial Term"), with two additional one (1) year option terms to be exercised by USAC in its sole discretion. The Initial Term of the awarded Contract shall commence on the effective date of the Contract ("Effective Date") as stated on the cover page.

## 7. SERVICES AND PRICES

The pricing used in the awarded Contract is based on the CLINs stated in this RFP. CLINs 001, 002 and 003 will be FFP, while CLIN 004 will be T&M pricing. Offerors may propose additional services in CLIN 004 to supplement the services included in Section B.10.

| CLIN | Description |
|---|---|
| 001 | IT Security Operation Center Services. Base Year (12 months). |
| 002 | IT Security Operation Center Services. First Option Year (12 months). |
| 003 | IT Security Operation Center Services. Second Option Year (12 months). |
| 004 | IT Security Additional Services. Optional CLIN |

## 8. USAC PROGRAM MANAGER AND CONTRACT ADMINISTRATOR

The Program Manager ("PM") for the awarded Contract is TBD. The PM may be contacted via email at TBD@usac.org. The USAC Contract Administrator ("CA") for the awarded Contract is TBD, who is the USAC point of contact for contractual matters (e.g. Contract administration, Contract modifications and other matters not related to performance). The CA may be contacted via email at TBD@usac.org.

## 9. PERFORMANCE REQUIREMENTS

Contractor shall begin performance of the Services and hold an awarded Contract kick-off meeting no later than five (5) business days following the Effective Date. During the awarded Contract kick-off meeting, Contractor shall present its notional project plan, as provided in Contractor's Contract proposal response ("Project Plan"). The Project Plan should be based on Contractor's past successful engagements and methodology for conducting support services of the type requested herein. Additionally, Contractor shall develop and present a final Project Plan ("Final Project Plan") within five (5) business days of the project kick-off meeting. Once USAC has approved the Final Project Plan, the plan shall then become the baseline for management of the overall project.

## 10. SCOPE OF SERVICES AND DELIVERABLES

### A. Scope of Services

Contractor is required to create a charter with the following:

- Overview
- Scope of the Engagement
- USAC Requirements
- Assumptions
- Deliverables
- Dependencies and Risks
- Project Timelines
- Success Factors and Measures
- Key Stakeholders
- Roles and Responsibilities
- Meeting Management
- Communication Plans

### B. Overview of Tasks Required

Contractor will:

1. Conduct security investigations based off alerts
2. Conduct daily threat hunting exercises
3. Develop knowledge base articles
4. Communicate investigations twice weekly and as needed to USAC staff
5. Incident Response Tabletop exercises (Yearly)
6. Participate in accreditations by proving audit artifacts
7. Provide shared management and support for USAC's Splunk environment

1. **Conduct Security Investigations**

Contractor will use security tools that USAC's Security Operations team have implemented in the environment. These well-known security tools are prevalent in the industry and are listed in Attachment 2. USAC will provide the licenses necessary to ensure Contractor Personnel can access USAC implemented systems.

Contractor will be expected to follow the following Service Level Agreement ("SLA") on alerting triage and remediation based on urgency of the event. The USAC Security Operations team takes a proactive and reactive strategy when it comes to the proposed SOC to be implemented. This allows USAC to be on the lookout for potential threats and help prevent threats in the future. Contractor must be able to provide resources that meet both requirements.

Reactive measures are investigations conducted by the SOC Team based on alerts and user reported concerns. Contractor will be required to review alerts generated by tools such as Security Information and Event Management ("SIEM") solution, Endpoint Detection & Response ("EDR"), vulnerability management, email protection, and others to investigate any threats to the organization. Any alert or user-based concern should be tracked by using USAC's ticketing system to ensure proper triage and documentation. The resources that are assigned to this Contract should have prior experience with ticketing systems and be detailed oriented when collecting evidence and documentation.

USAC has developed an incident response plan and procedure to outline reactive actions that need to be taken when reporting, triaging, and mitigating threats, or other activities. This plan and procedure indicate required actions including escalation paths and reporting requirements to ensure the organization is properly meeting the requirements called out its Memorandum of Understanding with the FCC. The Contractor Personnel assigned to this engagement will be required to follow the incident response plan and procedure with the assistance of the security analyst(s) on the USAC Security Operations team.

In addition to the incident response plan and procedure, USAC has implemented a SLA that Contractor will be required to meet during the review of alerts and user reported concerns. The SLAs outlined are to ensure potential threats to the organization are triaged in a reasonable time and have proper updates and associated documentation. Timelines in the SLAs are based on a 24/7 work schedule.

- 1 – Critical
  - Alerts that meet the critical classification will be assigned to an analyst within 1 hour of generation
  - A ticket will need to be opened and an initial triage will need to be conducted within that hour
  - Ticket needs to be updated with notes/actions taken every 3 hours after creation of the ticket
- 2 – High
  - Alerts that meet the high classification will be assigned to an analyst within 6 hours of generation

- A ticket will need to be opened and an initial triage will need to be conducted within those 6 hours
- Ticket needs to be updated with notes/actions taken every 12 hours after creation of the ticket

- 3 – Medium
  - Alerts that meet the medium classification will be assigned to an analyst within 24 hours of generation
  - A ticket will need to be opened and an initial triage will need to be conducted within those 24 hours
  - Ticket needs to be updated with notes/actions taken every 48 hours after creation of the ticket
- 4 – Low
  - Alerts that meet the low classification will be assigned to an analyst within 336 hours (2 weeks) of generation
  - A ticket will need to be opened and an initial triage will need to be conducted within those 336 hours (2 weeks)
  - Ticket needs to be updated with notes/actions taken every week after creation of the ticket
- 5 – Info
  - Not being brought in to ServiceNow as ticket

**2. Conduct Daily Threat Hunting Exercises**

From a proactive perspective, the Contractor Personnel will need to communicate frequently with USAC Security Operations staff to ensure a clear understanding of potential threats to USAC's network. Status updates should be provided at least twice a week and as needed for responding to incidents. USAC will provide a Webex link for Contractor to discuss the written report which will be emailed at the end of each meeting.

In addition to frequent communication, daily threat hunting activities should be conducted to proactively look for abnormal and suspicious behavior. This type of threat hunting activities must be documented in the way of investigations within USAC's Splunk system and activity that poses a high risk should be escalated to the USAC Security Operations Manager or designated point of contact. As previously noted, any ticket that is closed should have a knowledge base article attached to it to ensure future analysts can reference actions that should be taken.

**3. Develop Knowledge Base Articles**

Before a ticket can be closed out, the assigned Contractor Personnel will be required to link an existing knowledge base article to the ticket. This ensures other resources can review similar tickets and discover actions that should be taken for similar alert types. In the event no knowledge base articles exist pertaining to the current ticket, one should be created for future use within five (5) business days.

4. **Communicate Investigations Twice Weekly and As Needed to USAC Staff**

Additionally, twice monthly meetings (or more frequently as needed) shall occur with USAC IT leadership to present a summary of investigations, recommendations, and project updates. In the event there is a security incident or investigation of interest, Contractor will immediately reach out to the USAC Security Operations Manager or designated point of contact to communicate. If Contractor has a recommendation of a process change or a configuration change, Contractor should document the recommendation and address it with the USAC team at any time.

In the event there is an alert or user reported issue that is urgent in nature, the management team of Contractor will immediately reach out to the lead security analyst at USAC to ensure the proper awareness. The lead security analyst at USAC will provide guidance and escalate as needed.

5. **Incident Response Tabletop Exercises (Yearly)**

Contractor will plan and conduct an annual Incident Response Tabletop Exercise ("Tabletop Exercise"), in coordination with the USAC Privacy team and any other IT team the USAC Security Operations Manager or designated point of contact, to ensure that communication and incident handling is as effective and efficient as possible. Tabletop Exercises should include three or more scenarios of incidents that include privacy and/or cybersecurity related incidents. These scenarios will involve multiple departments within USAC and may include FCC personnel. Contractor is expected to provide a formal summary of the Tabletop Exercise as well as recommendations for improving Incident Response within 10 business days of the conclusion of the Tabletop Exercise.

6. **Participate In Accreditations by Proving Audit Artifacts**

Contractor must participate in accreditation interviews and various other audit activities to provide audit insight and artifacts regarding incident response when needed. USAC's Compliance team works with external security assessors and auditors to validate the organization has policy, procedures, and controls implemented in the appropriate manner to proactively protect the environment and meet the highest standards.

Contractor Personnel that are assigned to USAC will also need to show proof of training or proper certifications to use the tools USAC has implemented. This is intended to ensure a level of proficiency with the implemented technology and the concepts behind them. Key Personnel designated from Contractor are required to provide a list of certifications, education, and skills related to the execution of this contract.

7. **Provide Shared Management and Support for USAC's Splunk Environment**

USAC operates a Splunk cloud and relevant on-premises systems to support the Security Operations team. Contractor will be expected to provide support for USAC's Splunk environment, to include but not limited to enterprise security alert tuning, data input creation and normalization, and troubleshooting event collection issues. In addition, Contractor will be

expected to help with threat intelligence sources and general consultation for future roadmaps and expansions of the environment.

## C. DELIVERABLES

At a minimum, Contractor shall provide the deliverables listed in the table below. Offerors should also make recommendations as part of their proposal to this RFP submission on additional services or deliverables that might be needed out of the table below. These recommendations will be reviewed and considered during the proposal to this RFP evaluation and selection process.

All deliverables are considered Confidential Information (as defined in Section C.1.D.) and are the sole property of USAC. USAC may use and disclose the deliverables at its sole discretion. Each document deliverable shall be submitted in an acceptable format that is mutually agreed upon by USAC and Contractor.

| # | Frequency | Milestones / Deliverables | Description |
|---|---|---|---|
| 1 | One time (within 5 business days of Contract award) | Kickoff Meeting | Official kick-off of Contract to introduce team and approach as well as draft Project Plan. |
| 2 | One-time Plan (within five (5) business days of Contract award) | Onboarding Plan | Develop and submit a 60-day draft plan for onboarding all Contractor personnel and providing support for USAC teams and deliverables. |
| 3 | One-time Plan (within five (5) business days of Contract award) | Charter | Develop and submit an official charter that outlines the expectations from USAC and Contractor. |
| 4 | One-time (NLT 60 days before end of Contract period of performance) | Transition Plan | Develop and submit a 60-day plan for off boarding Contractor Personnel and providing support for USAC teams for the knowledge transfer of all deliverables and responsibilities. |
| 5 | Twice Weekly | Status Reports | Provide a written and oral overview of activities underway during current shift and activities needing continued activity. |
| 6 | Annually | Incident Response Tabletop Exercise | Exercise to test the USAC IT Security Operations team and organization's adherence to the incident response plan. |
| 7 | Annually | Incident Response Tabletop Exercise Lessons Learned | Documented recommendation as identified during the annual Incident Response Tabletop Exercise. |

| # | Frequency | Milestones / Deliverables | Description |
|---|---|---|---|
| 8 | Weekly | Threat Hunting Report | Report of threat hunting activities and results. |
| 9 | As Needed | Audit and Compliance Support | Provide artifacts and/or interview to support annual compliance and audit activities related to the execution of the Contract. |
| 10 | As Needed | Incident Investigations and Reporting | Conduct cybersecurity incident investigations and response as issues are detected; provide comprehensive details on the findings and recommendations related to the incident investigation. |
| 11 | One-time (with monthly update) | Deliverable Schedule | Develop and submit a proposed comprehensive deliverable schedule incorporating all deliverables contained in this section and when Contractor proposes these to be delivered. Proposed deliverable schedule to be presented for approval by USAC and reviewed at least monthly.<br>*Note: All deliverables need to be accompanied by a Deliverable Acceptance Form (or "DAF") in order to be formally accepted by USAC (see **Attachment 4**)* |
| 12 | As Needed | Status Report | Provide an informal consolidated update of all activities performed as well as planned activities |
| 13 | Quarterly | Quarterly Status Report | Provide a formal report of major/significant activities and accomplishments performed during the preceding month as well as planned major/significant activities for the subsequent month to be communicated to USAC leadership. |

## 11. MEETINGS, MANAGEMENT AND KEY PERSONNEL

### A. PROJECT KICK-OFF

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

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.

Contractor shall present the Project Plan to USAC for discussion. 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. USAC will approve the Project Plan within five (5) business days. All modifications and amendments to the awarded Contract must be approved in writing by an authorized USAC Procurement representative.

**B. TWICE WEEKLY STATUS MEETINGS**

Beginning five (5) business days after delivering the Final Project Plan to USAC, Key Personnel must schedule and participate in twice a week status meetings and travel to USAC's office in accordance with the requirements of the awarded Contract.

Contractor shall prepare a status report and submit it to USAC once per two weeks. 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 status report must include an expected completion date and the circumstances surrounding any possible delays. The status report shall be submitted one (1) business day before each regularly scheduled status meeting and no later than Friday noon (12:00 PM ET) during weeks in which the meeting is scheduled for Monday or when no status meeting is scheduled.

**C. MILESTONE STATUS MEETINGS**

Key Personnel must be prepared to present each deliverable either in-person or virtual via webcast meeting, as directed by USAC. For revision rounds, Key Personnel should be prepared to walk through any editing round questions via phone.

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

**D. ACCESSIBILITY**

Key Personnel must be accessible via telephone or email during USAC's normal business hours, Monday through Friday (9:00 AM - 6:00 PM ET) with availability from time to time prior to 9:00 AM and after 6:00 PM and on weekends if project activities and the needs of the business dictate the need for work outside of standard hours.

**E. MONTHLY STATUS REPORT ("MSR")**

Contractor's project manager for the awarded Contract shall prepare and send to USAC a MSR no later than the tenth ($10^{th}$) business day of each month. The MSR shall include the following:

1. Activities during each month by task (include on-going activities, new activities, activities completed; progress to date on all above-mentioned activities). Start each section with a brief description of the task.
2. Problems and corrective actions taken. Also, include issues or concerns and proposed resolutions to address them.

3. Personnel gains, losses, and personnel security status updates.
4. USAC IT Security Division required actions.
5. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
6. Accumulated invoiced cost up to the previous month.

## F. KEY PERSONNEL

The following are the minimum personnel who shall be designated as Key Personnel. USAC does not intend to dictate the size and composition of the ideal team to perform this Contract and expects offerors to provide an efficient and cost-effective teaming approach. However, USAC's understanding is that a team of 2-3 full time Contract Personnel per shift will provide the needed level of effort. Contractor shall provide staffing for the labor category below, or Contractor may propose other labor categories in its proposal to this RFP submission. 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. Any additional proposed labor categories to perform CLIN 004 must include the associated labor hour bill rate for each category submitted as well as the experience and qualifications of the personnel to be assigned to that labor category.

Minimum requirements for Key Personnel:

- Key Personnel provided on the awarded Contract should have the following certifications:
  - Splunk fundamentals 1, 2, and 3
  - CompTIA CYSA+
- Key Personnel provided on the awarded Contract must have a minimum of two years' experience in the following areas:
  - Experience with Windows and Linux event logs and malware intrusion detection
  - Threat intelligence
  - Demonstrated knowledge of threat hunting
  - Previous experience with ticketing systems
  - Basic understanding of networking of TCP/UDP, ports and protocols, Active Directory, and vulnerability management
  - High level understanding of scripting languages
- Ability to manage privacy related incidents

Contractor shall assign the following Key Personnel:

1. *Project Manager*. Contractor shall designate one (1) Key Personnel to be solely responsible for the customer delivery and satisfaction as the "Project Manager". This person has the authority to drive production, realign staff, and ensure delivery and timeliness of customer satisfaction. This person serves as a single point of contact for

USAC to relay priorities and business needs. The Project Manager ensures alignment and coordination among all functional areas.

Required capabilities shall include:

a. B.A. or B.S. degree or equivalent experience.
b. Minimum 5 years of experience in managing IT services with an emphasis on Agile and Project Management disciplines.

Desired capabilities shall include:

a. Experience and ability to coordinate and communicate project goals within customer environments, including the demonstrated ability to work with various organizational stakeholders to ensure proper involvement from management and technical teams.
b. Experience and ability to develop requirements from a project's inception to its conclusion for moderately complex situations.
c. Experience and ability to conduct assessments and develop recommendations that are reasonable and implementable given an organization's constraints.
d. Experience and ability distilling disparate bits of information into a coherent whole, and developing presentations/communications to support that coherent message.

All Key Personnel and other staff to support the awarded Contract must have employment background checks equal to those required by USAC for employees and contractors: education, national criminal, employment verification and social security verifications.

# SECTION C:

# USAC Terms and Conditions

## 1. DEFINITIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

W. "Derivative Works" means any and all modifications or enhancements to, or any new work based on, in whole or in part, any USAC Information, Confidential Information, Data, Software, or Deliverable regardless of whether such modifications, enhancements or new work is defined as a "derivative work" in the Copyright Act of 1976.

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

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

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

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

BB. "FIPS" means Federal Information Processing Standard.

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

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

EE. "IaaS" means Infrastructure as a Solution.

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

GG. "Malicious Code" or "Malware" means any software, firmware, program, routine, protocol, script, code, command, logic, or other feature that performs an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system and that is: (a) is designed to (i) disrupt, disable, deactivate, interfere with, or otherwise compromise USAC IT Systems, or (ii) access, modify, disclose, transmit, or delete PII, Data, Confidential Information, or USAC Information; or (b) either inadvertently or upon the occurrence of a certain event, compromises the confidentiality, integrity, privacy, security, or availability of PII, Data, Confidential Information, USAC Information, or USAC IT Systems. Examples of Malicious Code include, but are not limited to, viruses, worms, bugs, ransomware, spyware, bots, backdoors, devices, and Trojan Horses.

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

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

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

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

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

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

NN. "PaaS" means Platform as a Service.

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

PP. "Procurement Regulations" mean the following provisions of the Code of Federal Regulations: 2 C.F.R. §§ 200.318-321, 200-324, 200.326-327 and App. II to C.F.R. Part 200.

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

RR. "SaaS" means Software as a Service.

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

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

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

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

WW. "Software" means any application programming interface, content management system or any other computer programs, protocols, and commands that allow or cause a

computer to perform a specific operation or series of operations, together with all Derivative Works thereof.

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

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

ZZ. "USAC" means Universal Services Administrative Company.

AAA. "USAC Information" means any Data, materials, or communications in any form or format, whether tangible or intangible, spoken or written (regardless of media) provided by USAC to Contractor for use in the performance of the Contract, Data that is collected, developed or recorded by Contractor in the performance of the Contract, including without limitation, business and company personnel information, program procedures and program specific information, and Derivative Works thereof. All USAC Information is Confidential Information and subject to all requirements in Section 16 of these USAC Terms and Conditions.

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

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

DDD. "USF" means the Universal Service Fund.

## 2. TERM

The Initial Term is the period of time from the Effective Date (as defined in the 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 Terms and Conditions, below, and, in addition to any other remedies, may reduce the Contract price to deduct amounts for the defective work.

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

## 4. ENTIRE CONTRACT / BINDING EFFECT

The Contract supersedes and replaces all prior or contemporaneous representations, dealings, understandings or agreements, written or oral, regarding such subject matter. In the event of any conflict between these USAC Terms and Conditions and any other document made part of the Contract, the USAC Terms and Conditions shall supersede. Any waiver of any provision of the Contract will be effective only if in writing and signed by the party granting the waiver. The Contract shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and assignees.

## 5. MODIFICATIONS

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

## 6. INVOICES

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

CoupaHelp@usac.org. For assistance on all non-Coupa related billing questions, Contractor may email accounting@usac.org.

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

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

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

## 7. FEES AND RATES INCLUSIVE OF ALL CHARGES AND TAXES

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

## 8. PAYMENT

Contractor shall be paid for Services performed on a fixed-price, service category rate basis using the service categories and fixed rates set forth in **Attachment 1**. USAC will pay invoices submitted in accordance with Section 6 of these USAC Terms and Conditions within thirty (30) calendar days of receipt of invoice, provided the Services and/or Deliverables have been delivered and accepted by USAC.

## 9. ASSIGNMENT, DELEGATION, AND SUBCONTRACTING

Contractor shall not assign, delegate, or subcontract all or any portion of the Contract without obtaining USAC's prior written consent. Consent must be obtained at least thirty (30) days prior to the proposed assignment, delegation, or subcontracting. USAC may require information and assurances that the proposed assignee, 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 Personnel to stop work, to the extent specified in said notice; and (b) subject to the prior written approval of USAC, transfer title and/or applicable licenses to use, as appropriate, to USAC and deliver to USAC, or as directed by USAC, all USAC Information, Confidential Information, Data, Software, Deliverable, or any Derivative Work to any of the preceding, whether completed or in process, for the work stopped. In the event of a stop work order, all deadlines in the Contract shall be extended on a day for day basis from such date, plus reasonable additional time, as agreed upon between the parties, acting in good faith, to allow Contractor to reconstitute its staff and resume the work.

## 14. LIMITATION OF LIABILITY

Except in cases of gross negligence or willful misconduct, in no event shall USAC be liable for any consequential, special, incidental, indirect or punitive damages arising under or relating to the performance of the Contract. USAC's entire cumulative liability from any causes whatsoever, and regardless of the form of action or actions, whether in contract, warranty, or tort (including negligence), arising under the Contract shall in no event exceed the aggregate amount paid by USAC to Contractor in the year preceding the most recent of such claims. All exclusions or limitations of damages contained in the Contract, including, without limitation, the provisions of this Section, shall survive expiration or termination of the Contract.

## 15. INDEMNITY

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

## 16. CONFIDENTIAL INFORMATION

A. *Confidential Information*. Confidential Information includes, but is not limited to, USAC Information, Data, materials, or communications in any form or format, whether tangible or intangible, spoken or written (regardless of media) that contains, reflects, or is derived from or based upon, or is related to:

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

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

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

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

5. Information compiled, prepared or developed by Contractor in the performance of the Contract;

6. PII; and

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

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

C. *Sub-Recipient Access to Confidential Information*. Recipient shall not disclose Confidential Information to a Sub-Recipient unless absolutely necessary for a Recipient's or Sub-Recipient's performance of the Contract, and if necessary, shall only disclose the Confidential Information necessary for Sub-Recipient's performance of its duties. As a pre-condition to access to Confidential Information, Recipient shall require Sub-Recipients, including Contractor Personnel to sign a non-disclosure or confidentiality agreement containing terms no less restrictive than those set forth herein. Discloser may enforce such agreements, if necessary, as a third-party beneficiary.

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

E. *Exclusions*. If requested to disclose Confidential Information by an authorized governmental or judicial body, Recipient must promptly notify Discloser of the request and to the extent that it may legally do so, Recipient must refrain from disclosure of the Confidential Information until Discloser has had sufficient time to take any action as it deems appropriate to protect the Confidential Information. In the event Confidential Information of USAC is requested, Recipient must immediately notify USAC, with a copy to USAC's General Counsel, of the request. Neither Contractor nor Contractor Personnel shall issue any public statement relating to or in any way disclosing any aspect

of the Contract without the prior written consent of USAC. Notwithstanding anything herein to the contrary, USAC may, without notice to Contractor, provide the Contract, including Contractor's proposal information, and any information or Data delivered, prepared or developed by Contractor in the performance of the Contract to the FCC or other governmental or judicial body, and may publicly disclose basic information regarding the Contract, e.g., name of Contractor, price, basis for selection, description of Services/Deliverables and any provisions necessary for USAC to justify actions taken with respect to the Contract.

## 17. RETURN OR DESTRUCTION OF USAC INFORMATION

A. *Return or Destruction of USAC Information.* Except as provided in Section 17.B of these USAC Terms and Conditions, and promptly upon the expiration or termination of the Contract (or such earlier time as USAC may direct), Contractor shall, at the direction of USAC, and at no additional cost to USAC, return or destroy all USAC Information, including all copies thereof, in the possession or under the control of Contractor or Contractor Personnel. If USAC directs that Contractor destroy any USAC Information, then, at USAC's request, Contractor shall provide USAC with an executed certificate in writing stating that all such USAC Information was destroyed.

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

C. *No Withholding of USAC* Information. Contractor shall not withhold any USAC Information as a means of resolving any dispute. To the extent that there is a dispute between Contractor and USAC, Contractor may make a copy of such USAC Information as is necessary and relevant to resolution of the dispute. Any such copies shall promptly be destroyed upon resolution of the dispute.

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

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

F. *No Other Use.* USAC Information is provided to Contractor solely for the purpose of rendering the Services, and USAC Information or any part thereof shall not be sold, assigned, leased, or otherwise transferred to any third party by Contractor (except as required to perform the Services or as otherwise authorized in the Contract), commingled

with non-USAC Information, modified, decompiled, reverse engineered, or commercially exploited by or on behalf of Contractor, Contractor Personnel, or any third party.

## 18. INFORMATION SECURITY

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

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

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

D. *Integration.* Prior to delivering the Services/Deliverables or enabling data-sharing or interoperability of any kind with USAC IT Systems, Contractor shall: (i) work with USAC to document, establish and enable the effective and secure integration of any gateways or data transmission mechanisms necessary for the parties to perform their obligations under the Data Security Laws; (ii) complete any security questionnaires, IT rules of behavior,

certifications, assessments, or workforce training reasonably requested by USAC in a timely manner; and (iii) receive prior written authorization from USAC to access USAC 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 or Deliverables, their establishment shall be at Contractor's sole cost and expense. Under no circumstances shall USAC's written authorization to access its IT System serve as a representation or warranty by USAC that such access is secure or as a waiver of these USAC Terms and Conditions. Failure to satisfy the conditions set forth in subsections (i) – (iii) herein to USAC's reasonable satisfaction shall be considered a material breach of the Contract by Contractor.

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

F. *Access to PII, Data, USAC Information, USAC Confidential Information and USAC IT Systems.* Contractor agrees that access to the PII, Data, USAC Information, USAC Confidential Information, and USAC IT Systems is at USAC's sole discretion, and that Contractor's access to such system or information may be conditioned, revoked or denied by USAC at any time, for any reason, without any liability whatsoever to USAC. Access to USAC IT Systems by Contractor and Contractor Personnel, including any data-sharing or interoperability between USAC and Contractor, shall be for the sole purpose of providing the Services or Deliverables. Contractor agrees that: (i) USAC IT Systems is owned solely by USAC; (ii) USAC will monitor the use of USAC IT Systems; (iii) neither Contractor nor Contractor Personnel 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 USAC Confidential Information, as defined by these USAC Terms and Conditions. Contractor will not use USAC IT Systems except as expressly authorized by USAC. USAC may require that Contractor Personnel use a USAC.org email address when providing Services. Contractor agrees that its use of, and access to, USAC IT Systems is completely at its own risk.

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

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

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

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

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

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

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

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

## 19. SECURITY INCIDENTS AND DATA BREACHES

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

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

C. *Mitigation and Elimination Efforts.* Contractor, working with USAC, shall use its best efforts to mitigate and eliminate the effects of the Security Incident or Data Breach on USAC and, if the Security Incident or Data Breach causes any loss of operational efficiency, loss of data, or unauthorized disclosure, Contractor will assist USAC in mitigating or restoring such losses or disclosures. Contractor agrees to fully cooperate with USAC in the investigation of the Security Incident or Data Breach and to participate in, to the extent directed by USAC, the notification of individuals, the media, the FCC, or third parties. Contractor shall promptly respond to USAC's questions regarding the Security Incident or Data Breach and coordinate with Contractor Personnel if required to mitigate the harm. To the extent USAC determines necessary, USAC agrees to provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. Notwithstanding anything to the contrary in the

Contract, if the Security Incident or Data Breach is due to the negligence or misconduct of Contractor or Contractor Personnel, then Contractor shall: (i) perform its obligations under this Section at no cost to USAC; (ii) promptly implement or develop any additional protocols, policies, gateways, transmission mechanisms, or security layers, if reasonably necessary, at its sole cost and expense, and with the approval of USAC; (iii) indemnify USAC for all damages, and if needed PII, USAC Information, USAC Confidential Information, Data, and USAC IT Systems breach mitigations, under this Section as a result of the Security Incident or Data Breach. Failure to strictly abide by these USAC Terms and Conditions shall be considered a material breach of the Contract for which USAC shall have the right to immediately terminate for cause.

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

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

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

## 20. MALICIOUS CODE AND MALICIOUS CYBER ACTIVITIES

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

Contractor will not introduce Malicious Code into USAC IT Systems or engage in Malicious Cyber Activities in, with, or involving the Services or USAC IT Systems. For any aspect of the

Services in Contractor's IT Systems, Contractor will comply with NIST SP 800-83 Rev. 1 or the most current revision thereof to prevent Malicious Code. Contractor will perform regularly scheduled (preferably in real-time, but in no event less frequently than daily) virus checks using the latest commercially available, most comprehensive virus detection and scanning programs. If Contractor becomes aware that any Malicious Code has been introduced into any USAC IT System, or that Contractor has engaged in Malicious Cyber Activities, Contractor will notify USAC immediately. In addition, Contractor will use its best efforts to assist USAC in reducing the effects of the Malicious Code or Malicious Cyber Activities and, if the Malicious Code or Malicious Cyber Activity causes a loss of operational efficiency or loss of data, to assist USAC in mitigating and restoring such losses. USAC will provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. If Malicious Code is found to have been introduced into any USAC IT System or the Services, Contractor will perform all of its obligations under this Section at no cost to USAC, and Contractor will be liable to USAC for damages and costs incurred by USAC as a result of such Malicious Code. If Contractor or Contractor Personnel has been found to (a) have engaged in any Malicious Cyber Activities; or (b) have allowed Malicious Cyber Activities to have occurred due to its willful, reckless, or negligent actions or omissions, Contractor will be liable to USAC for damages and costs incurred by USAC as a result of such Malicious Cyber Activities.

The introduction of Malicious Code into USAC IT Systems, and/or the engaging in Malicious Cyber Activity involving USAC IT Systems, shall be considered a Data Breach. If Contractor becomes aware that Malicious Code has been introduced into USAC IT Systems, or Contractor has engaged in Malicious Cyber Activity, Contractor will notify USAC in writing within the time frame required by the United States Computer Emergency Readiness Team and the FCC, which is currently within one (1) hour and otherwise act in a manner consistent with Section 19 of these USAC Terms and Conditions.

## 21. FISMA PROVISIONS

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

**Safeguarding of Contractor IT Systems:**

USAC's security strategy for Data includes the requirement to ensure the security of protection controls for Data regardless of the location or the party responsible for those controls. Contractor acknowledges that it serves a vital role in achieving this goal. Contractor shall apply the following minimum safeguarding requirements and procedures from NIST SP 800-171 Revision 2 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" to protect covered Contractor IT Systems and USAC Data. Contractor shall, upon request, provide USAC with copies of its security policies and procedures to review. USAC may require a written response that may be an attestation of compliance, a submission of supporting document, or both. If USAC requests such a written response, Contractor shall submit an electronic copy of the document(s) confirming compliance within ten (10) calendar days. If there are any requirements

that are out of scope or that cannot be complied with, Contractor shall fully explain those requirements with a business justification to USAC. Contractor must be in compliance with all such requirements unless USAC agrees in writing with Contractor that Contractor does not have to comply. If Contractor is not in compliance with all requirements and has not received written confirmation from USAC that Contractor may not comply with a requirement, USAC may terminate this Contract immediately upon written notice to Contractor.

Contractor shall:

A. Limit Contractor IT Systems access to only authorized USAC employees and contractors, authorized Contractor Personnel and authorized processes.
B. Limit Contractor IT Systems access to only the types of transactions and functions that USAC employees and contractors and authorized Contractor Personnel are permitted to execute.
C. Verify and control/limit connections to and use of external Contactor IT Systems.
D. Control information posted or processed on publicly accessible Contractor IT Systems.
E. Sanitize or destroy Contractor IT Systems media containing USAC Information as described in Section 17.C. of these USAC Terms and Conditions.
F. Limit physical access to Contractor IT Systems, equipment, and the respective operating environments to only USAC employees and contractors and authorized Contractor Personnel.
G. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
H. Monitor, control, and protect Contractor organizational communications (i.e., information transmitted or received by Contractor IT Systems) at the external boundaries and key internal boundaries of the Contractor IT Systems.
I. Implement subnetworks for publicly accessible Contractor IT Systems components that are physically or logically separated from internal networks.
J. Identify, report, and correct information and Contractor IT Systems flaws promptly.
K. Provide protection from Malicious Code at appropriate locations within Contractor IT Systems.
L. Update Malicious Code protection mechanisms when new releases are available.
M. Perform periodic scans (no less frequently than daily) of Contractor's IT Systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

## 22. TECHNOLOGY CONSIDERATIONS

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

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

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

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

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

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

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

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

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

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

## 23. PROPRIETARY RIGHTS

Contractor agrees that all Data, Software, Deliverables, and all Derivative Works thereof are USAC property and shall be deemed USAC Information and are works made-for-hire for USAC within the meaning of the copyright laws of the United States. In the event that any of the aforementioned are not considered works made-for-hire for USAC within the meaning of the copyright laws of the United States, Contractor shall and hereby does irrevocably grant, assign, transfer and set over unto USAC in perpetuity all worldwide rights, title and interest of any kind, nature or description it has or may have in the future in and to such materials, and Contractor shall not be entitled to make any use of such materials beyond what may be described in this Contract.

Contractor hereby waives, and shall secure waiver from Contractor Personnel any moral rights in such assigned materials, such as the right to be named as author, the right to modify, the right to prevent mutilation and the right to prevent commercial exploitation. Accordingly, USAC shall be the sole and exclusive owner for all purposes for the worldwide use, distribution, exhibition, advertising and exploitation of such materials or any part of them in any way and in all media and by all means.

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

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

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

## 24. RESPONSIBILITY FOR CONTRACTOR PERSONNEL

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

Contractor Personnel requiring access to USAC IT Systems will be required to sign USAC's IT Security Rules of Behavior Form and complete mandatory IT Security and Privacy Awareness Online Training before being given access to USAC IT Systems. Contractor may be required to complete Role-Based Privacy Act Training, at Contractor's own cost, if accessing USAC information systems designated as federal systems of record.

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

## 25. KEY PERSONNEL

USAC may specify which Contractor employees are Key Personnel under the Contract. Key Personnel assigned to the Contract must remain in their respective positions throughout the Contract Term. USAC may terminate all or a part of the Contract if Contractor changes the position, role, or time commitment of Key Personnel, or removes Key Personnel from the Contract, without USAC's prior written approval. USAC may grant approval for changes in staffing of Key Personnel if it determines in its sole discretion, that:

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

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

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

## 26. SHIPMENT/DELIVERY

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

## 27. INSURANCE

At its own expense, Contractor shall maintain sufficient insurance in amounts required by law or appropriate for the industry, whichever is greater, to protect and compensate USAC from all claims, risks and damages/injuries that may arise under the Contract, including, as appropriate, worker's compensation, employer's liability, commercial general liability, commercial crime coverage, automobile liability, professional liability, cyber liability (which may be included in some professional liability coverage), and excess / umbrella insurance. Upon USAC's request, Contractor shall name USAC as an additional insured to those insurance policies that allow it.

Upon USAC's request, Contractor shall cause its insurers to waive their rights of subrogation against USAC. Contractor shall produce evidence of such insurance upon request by USAC. If the insurance coverage is provided on a claims-made basis, then it must be maintained for a period of not less than three (3) years after acceptance of the Deliverables and/or Services provided in connection with this Contract. Contractor shall provide written notice thirty (30) days prior to USAC in the event of cancellation of or material change in the policy.

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

## 28. CONFLICTS OF INTEREST

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

## 29. WAIVER

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

## 30. SEVERABILITY

The invalidity or unenforceability of any provisions of the Contract shall not affect the validity or enforceability of any other provision of the Contract, which shall remain in full force and effect. The parties further agree to negotiate replacement provisions for any unenforceable term that are

as close as possible to the original term and to change such original term only to the extent necessary to render the same valid and enforceable.

## 31. CHOICE OF LAW / CONSENT TO JURISDICTION

The Contract shall be governed by and construed in accordance with the laws of the District of Columbia without regard to any otherwise applicable principle of conflicts of laws. Contractor agrees that all actions or proceedings arising in connection with the Contract shall be litigated exclusively in Courts. This choice of venue is intended to be mandatory and the parties waive any right to assert forum non conveniens or similar objection to venue. Each party hereby consents to in personam jurisdiction in the Courts. Contractor must submit all claims or other disputes to the procurement specialist and USAC General Counsel for informal resolution prior to initiating any action in the Courts and must work with USAC in good faith to resolve any disputed issues. If any disputed issue by Contractor is not resolved after thirty (30) calendar days of good faith attempts to resolve it, Contractor may instigate legal proceedings. A dispute over payment or performance, whether informal or in the Courts, shall not relieve Contractor of its obligation to continue performance of the Contract and Contractor shall proceed diligently with performance during any dispute over performance or payment.

## 32. USAC AND APPLICABLE LAWS

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

## 33. RIGHTS IN THE EVENT OF BANKRUPTCY

All licenses or other rights granted under or pursuant to the Contract are, and shall otherwise be deemed to be, for purposes of Section 365(n) of the Code, licenses to rights to "intellectual property" as defined in the Code. The parties agree that USAC, as licensee of such rights under Contractor, shall retain and may fully exercise all of its rights and elections under the Code. The parties further agree that, in the event of the commencement of bankruptcy proceedings by or against Contractor under the Code, USAC shall be entitled to retain all of its rights under the

Contract and shall not, as a result of such proceedings, forfeit its rights to any Data, Software, Deliverable, or any Derivative Work thereof.

## 34. NON EXCLUSIVITY

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

## 35. INDEPENDENT CONTRACTOR

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

## 36. TEMPORARY EXTENSION OF SERVICES

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

## 37. NOTICES

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

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

*If to USAC*:
Chief Administrative Officer, Universal Service Administrative Company
700 12th Street, NW, Suite 900
Washington, DC 20005
Email: To the designated USAC Contract Officer for this procurement, with a copy to usacprocurement@usac.org.

With a copy to:

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

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

## 38. SURVIVAL

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

## 39. FORCE MAJEURE

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

## 40. EXECUTION / AUTHORITY

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

## 41. SECTION 508 STANDARDS

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

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

## 42. NATIONAL SECURITY SUPPLY CHAIN REQUIREMENTS

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

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

**B.** *Prohibition*. Contractor will ensure that no funds from USAC or other federal subsidies under this Contract will be used to purchase, obtain, maintain, or otherwise support any equipment or services produced or provided by a Covered Company. Contractor must also ensure that no funds administered by USAC or the FCC under this Contract will be used to purchase, obtain, maintain or otherwise support Covered Equipment or Services placed on the Covered List. These prohibitions extend to any subcontractors that provides Services under the Contract.

Contractor is responsible for notifying any subcontractors it engages under this Contract of this prohibition.

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

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

(i) If for equipment produced or provided by a Covered Company or equipment on the Covered List:
   a. The Covered Company that produced the equipment (include entity name, unique entity identifier, CAGE code, and whether the Covered Company was the original equipment manufacturer ("OEM") or a distributor, if known);
   b. A description of all equipment (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and
   c. Explanation of the why USAC funds purchased, obtained, maintained, or otherwise supported the equipment and a plan to remove and replace such equipment as expeditiously as possible.

(ii) If for services produced or provided by a Covered Company or services on the Covered List:
   a. If the service is related to item maintenance: A description of all such services provided (include on the item being maintained: brand; model number, such as

OEM number, manufacturer part number, or wholesaler number; and item description, as applicable);

i. If the service is not associated with maintenance, the product service code of the service being provided; and

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

Contractor shall retain audit ready supporting evidence for all certifications.

## 43. ADDED SERVICES

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

## 44. ADEQUATE COVID-19 SAFETY PROTOCOLS

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

To provide adequate COVID-19 safeguards for USAC employees, Contractor shall ensure that all Contractor Personnel that enter USAC premises will comply with USAC's COVID-19 Vaccination Validation & Testing 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.

# SECTION D:

# Attachments

Attachment List:

- Attachment 1: Bid Sheet
- Attachment 2: USAC Security Tools
- Attachment 3: USAC Confidentiality Agreement
- Attachment 4: Deliverable Acceptable 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 and USAC Terms and Conditions set forth in RFP sections A, B, C, and D and any attachments listed in section D (hereafter collectively referred to as the "Terms and Conditions"). Offeror's submission of a proposal constitutes its agreement to the Terms and Conditions and their precedence over any other terms, requirements, or conditions proposed by Offeror.

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

### B. PERIOD FOR ACCEPTANCE OF OFFERS

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 the Statement of Work (Section B), and should not contain a significant amount of corporate boilerplate marketing information.
- Be submitted to USAC Procurement Department, **no later than 11:00 AM ET on May ~~9~~17, 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-23-064, 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 |
|---|---|
| April 6, 2023 | RFP Released |
| April 17, 2023 | Questions Due to USAC by 11:00 AM ET at rfp@usac.org |
| April 20, 2023 | Q&A Released to Potential Offerors |
| May 3, 2023 | Virtual Bidder's Conference |
| May ~~9~~17, 2023 | Proposal Due to USAC by 11:00 AM ET at rfp@usac.org |
| August 2023 | Anticipated Award Date |

Due to the importance of this procurement and USAC's desire to ensure that potential bidders have all the relevant information available to respond to this solicitation, USAC will host a 1-hour Bidder's Conference on May 3, 2023 from 11:00 AM to 12:00 PM where USAC will further discuss the requirements of this solicitation and provide answers to questions. To attend the Bidder's Conference, potential bidders must email their list attendees and email addresses to rfp@usac.org. USAC will promptly review each request and will notify the potential bidder with the conference information.

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 **April 17, 2023, 11:00 AM ET**. USAC plans to post all questions and responses under this procurement on our website by **April 20, 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 award a contract after all steps in the procurement process have taken place. 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 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 proposal volume 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 I)

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*. 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.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 II)**

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

Note: Offers that include material 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 III)

This volume must include:

1. A cover page, as outlined above.

2. Description of Offeror's experience with consultation and support of an organization's information security program of similar size and scope. Provide examples of the projects and personnel to include types of positions and length of assignments.

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 IV)

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.

2. Page Limitation

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

   a. Volume I – Corporate Information; may not exceed four (4) pages, including cover page.

   b. Volume II – Technical; may not exceed fifteen (15) pages; however, excluding **Appendix A** (Resumes).

   c. Volume III – Past Performance Information; may not exceed five (5) pages, including cover page.

   d. Volume IV – Price; may not exceed four (4) pages, including cover page.

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.

- **Technical:** The technical sub-factors listed below in descending order of importance:
  a. Technical Approach
  b. Capabilities
  c. Key Personnel

- **Past Performance**: 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 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 the Offeror's proposal that are not identified as references).

- **Price Evaluation**: USAC will evaluate price based on proposed pricing methodology, 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 services 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 Services described in this RFP 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 this 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, 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 attachment]

# Attachment 2

## USAC Security Tools

USAC Operations Team uses the following tools to monitor and alert in the environment:

- Splunk Enterprise Security
- Carbon Black EDR
- Proofpoint
- Rapid 7 Insight VM

# 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** | |