USAC Solicitation for Enterprise Cybersecurity and Monitoring Services – 1st Revision

SOLICITATION INFORMATION:

Method of Solicitation:	Request for Proposal ("RFP")
Contract Period of Performance:	One (1) Base Year plus Four (4) Option Years
Solicitation Number:	IT-26-073
Solicitation Issue Date:	April 27, 2026
Question Due Date:	May 11, 2026 by 11:00 AM ET
Proposal Due Date:	June 10, 2026 by 11:00 AM ET

CONTRACT TO BE ISSUED BY:

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

CONTACT INFORMATION:

USAC CONTACT INFORMATION	OFFEROR CONTACT INFORMATION
Anthony Smith Senior Procurement Specialist P: 202-916-3486 Email: Procurement@usac.org and Anthony.Smith@usac.org	(complete) Name: _____ POC: _____ POC Title: _____ POC Phone: _____ POC Email: _____ Address: _____

SECTION A: About Us

1. ABOUT USAC

Through its administration of the Universal Service Fund ("USF") programs on behalf of the Federal Communications Commission ("FCC"), the Universal Service Administrative Company ("USAC") works to promote the availability of quality telecommunications services at just, reasonable, and affordable rates, and to increase access to advanced telecommunications services throughout the nation. Specifically, the USF programs provide funding for the expansion of telecommunications and broadband access to rural communities and health care facilities, schools and libraries, and low-income households. Through program administration, auditing, and outreach, USAC works with contributors, service providers, and program beneficiaries to achieve the program goals articulated by the FCC for the High Cost Program, Lifeline Program, Rural Health Care Program, and Schools and Libraries Program.

USAC strives to provide efficient, responsible stewardship of the programs, each of which is a key national asset in making important telecommunications and Internet services available to consumers, health care providers, schools, and libraries throughout the United States. The program divisions are supported by additional USAC personnel in other divisions, including Finance, Office of General Counsel ("OGC"), Information Systems, Audit and Assurance, Enterprise Process Improvement ("EPI"), and Human Resources ("HR").

Consistent with FCC rules, USAC does not make policy nor interpret unclear provisions of statutes or the FCC's rules. The USF is funded by contributions from telecommunications carriers, including wireline and wireless companies, and contributions from interconnected voice over internet protocol ("VoIP") providers, including cable companies that provide voice service, based on an assessment of their interstate and international end-user revenues. These contributions are typically passed through to consumers through a universal service fee line item on their telephone bills.

High Cost Program

The High Cost Program is designed to ensure that consumers in rural, insular, and high-cost areas have access to modern communications networks capable of providing voice and broadband service, both fixed and mobile, at rates that are reasonably comparable to those in urban areas ("High Cost"). High Cost fulfills this universal service goal by allowing eligible carriers who serve these areas to recover some of their costs from the USF. Like all USF programs, the administration of High Cost has undergone significant modernization in the last several years to increase innovation and ensure beneficiaries have access to updated technology. USAC developed and now leverages the High Cost Universal Broadband Portal ("HUBB"), which allows participating carriers to file deployment data showing where they are building out mass-market, high-speed internet service by precise location. This information includes latitude and longitude coordinates for every location where service is available, and USAC displays this information on a public-facing map to show the impact of high-cost funding on broadband expansion throughout the United States.

Lifeline Program

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

Rural Health Care Program

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

Schools and Libraries Program (E-Rate)

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

Contributions

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

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

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

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

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

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

2. 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 (as defined in Section C.1.D of this RFP) 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. CONFIDENTIALITY

This RFP is subject to the terms of the Confidentiality Agreement (attached hereto as **Attachment 2**) which must be executed by Offeror and submitted along with any proposal for this RFP. Any contract for awarded work under this RFP will also be subject to the terms of such Confidentiality Agreement.

4. OFFEROR AND CONTRACTOR DESIGNATION

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".

SECTION B:
Statement of Work

1. OVERVIEW

Contractor shall provide enterprise cybersecurity and network monitoring support services in support of USAC's information security, network operations, compliance, risk management, and continuous monitoring objectives. Contractor shall furnish all management, supervision, labor, processes, and associated support necessary to provide integrated cybersecurity and network monitoring services in a managed services model, in accordance with the requirements of this Section B: Statement of Work.

2. TYPE OF CONTRACT

The contract to be awarded pursuant to this RFP will either be a single-award contract ("Contract") or multiple-award Contracts. USAC intends to award a Contract to the responsible Offeror whose proposal represents the best overall value. USAC may award a single contract for all task areas or separate contracts for each task area if USAC determines multiple contract awards provide the best overall value. The awarded Contract(s) will have a hybrid firm fixed price ("FFP") and time and materials ("T&M") with a not-to-exceed ("NTE") ceiling price set forth in **Attachment 1: Bid Sheet**. CLINs 0001, 0002 and 0003 will be FFP, while CLINs 0004 and 0005 will be T&M pricing. The FFP and fixed labor rates for T&M pricing are to include all direct and indirect costs set forth in this Section B, including equipment, product support, supplies, general and administrative expenses, overhead, materials, travel, labor, taxes (including use and sales taxes), shipping, and profit. USAC will not reimburse Contractor for any travel-related expenses.

Offerors must provide separate pricing in **Attachment 1: Bid Sheet** for each CLIN as follows:

CLIN #	Description	Pricing Method
0001	**Task Area 1:** Security Compliance, Vulnerability Management, and Risk Support	FFP
0002	**Task Area 2:** Integrated 24x7x365 Security Operations Center and Network Operations Center Support	FFP
0003	**Task Area 3**: Security Engineering, SIEM, and Enterprise Monitoring Support	FFP
0004	**Task Area 4**: Security Architecture and Emerging Cybersecurity Capabilities	T&M including an annual NTE
0005	**Task Area 5**: Program Management, Reporting, Performance Management, and Transition Support for Task Areas 1 - 4	T&M including an annual NTE
0006	Overall NTE to deliver all five (5) Task Areas (CLINs 0001 – 0005)	To be presented as an overall NTE

3. CONTRACT TERM

The term of this Contract shall be for a base period of one (1) year with four (4) one-year renewal options ("Contract Term"), unless extended by USAC or terminated sooner in accordance with the Contract. The Contract Term shall commence on the first day of the awarded Contract period of performance (the "Effective Date") as set forth in the awarded Contract. ~~USAC may award task orders at any time during the Contract Term. The performance period of each awarded task order will be stated within the awarded task order. USAC anticipates that the awarded task order performance period will be within the Contract Term, but the performance period may extend beyond the Contract Term in accordance with this section.~~

4. PLACE OF PERFORMANCE

4.1 All required Services (as defined in Section C.1.U) under the awarded Contract must be performed within the United States at either USAC's headquarters at 700 12th Street NW, Suite 900, Washington, DC 20005 ("USAC Headquarters"), virtually, or such other location as USAC may approve in its sole discretion. Presently, USAC has a hybrid work approach requiring Contractor Staff (as defined in Section C.1.G) to be in the USAC office at least 2 days per week. Contractors that are required to report in person must reserve their workspaces in designated areas in advance using USAC's hoteling system.

4.2 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.

4.3 Contractor shall schedule, coordinate, and hold a Contract "Kick-Off Meeting" (as described in this section and Section B.8) no later than ten (10) workdays after any Contract award, at USAC Headquarters or virtually as approved by USAC. The Kick-Off Meeting will provide an introduction between Contractor Staff and USAC personnel who will be involved with the awarded Contract. The meeting will provide the opportunity to discuss technical, management, and security issues, and review Contractor's proposed project timeline and reporting procedures. At a minimum, the attendees shall include Key Personnel (as described in Section C.1.N), Contractor Staff capable of obligating Contractor, and USAC personnel.

4.4 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 any USAC information systems designated as a federal system of records (i.e., National Verifier and National Lifeline Accountability Database).**

4.5 Status update meetings and other meetings may be held virtually, except to the extent that USAC or Contractor requires in-person presence and will be held in accordance with USAC and Contractor Continuity of Operations Plan ("COOP"). While attending USAC

Headquarters for meetings or to conduct audits, Contractor Staff will be considered as visitors. All visitors are required to complete USAC's Visitor Form, and wear a badge while on premises. The Kick-Off Meeting and all in-person meetings will be held at USAC Headquarters or other reasonable locations designated by USAC. Contractor may also be required to attend meetings at the FCC offices located at 45 L Street NE Washington, DC 20554.

4.6 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 or system/software is down.

5. SCOPE OF WORK

Contractor shall provide enterprise cybersecurity and network monitoring support services in support of USAC's information security, network operations, compliance, risk management, and continuous monitoring objectives. Contractor shall furnish all management, supervision, labor, processes, and associated support necessary to provide integrated cybersecurity and network monitoring services in a managed services model, in accordance with the requirements of this Section B: Statement of Work.

Contractor shall provide support across enterprise cybersecurity and network monitoring functional areas, including, but not limited to, security compliance support, Information System Security Officer ("ISSO") support, vulnerability management, IT risk support, Security Architecture, 24x7x365 Security Operations Center ("SOC") support, 24x7x365 Network Operations Center ("NOC") support, security engineering support, Security Information and Event Management ("SIEM") support, enterprise monitoring support, Supply Chain Risk Management ("SCRM"), artificial intelligence ("AI") security support, program management, reporting, performance management, and transition support.

Contractor shall perform services necessary to support the organization's ability to monitor, detect, analyze, respond to, report on, and continuously improve its handling of cybersecurity and network events affecting enterprise systems, services, applications, and infrastructure. Contractor shall support secure and reliable enterprise operations through coordinated cyber defense, network awareness, security compliance activities, risk-informed decision support, and technical engineering services.

Contractor shall provide services in a manner that supports continuous situational awareness, timely reporting, measurable performance, documented operational procedures, and a structured service delivery model. Contractor shall provide all required deliverables, reports, dashboards, metrics, and management artifacts necessary for the organization to oversee performance and maintain continuity of operations.

Contractor shall perform all work in accordance with applicable laws, directives, standards, and guidance identified in this Section B: Statement of Work. Services shall be delivered using

generally accepted cybersecurity, engineering, operational, and program management practices appropriate to a formal government procurement environment.

6. TASK AREAS

6.1 Task Area 1: Security Compliance, Vulnerability Management, and Risk Support

6.1.1 Contractor shall provide integrated security compliance, vulnerability management, and risk support services necessary to maintain and enhance the organization's cybersecurity governance, authorization posture, continuous monitoring activities, and risk-informed decision-making processes.

6.1.2 Contractor shall provide ISSO support for the strategic and day-to-day execution of security compliance and authorization activities. Support shall include the development, maintenance, coordination, and update of required security documentation and security artifacts associated with security authorization, ongoing security authorization, risk management, and security compliance activities. Such support may include, but is not limited to, system security documentation, inventories, contingency-related documentation, risk assessment support, control implementation support, review of system categorizations, and coordination with stakeholders responsible for security, privacy, technology, and operations.

6.1.3 Contractor shall support the lifecycle activities associated with the Risk Management Framework ("RMF"), Assessment and Authorization ("A&A"), and continued authorization processes, including support for systems undergoing new authorization, reauthorization, or ongoing security authorization activities. Contractor shall assist in maintaining authorization posture, identifying compliance gaps, coordinating security documentation updates, supporting control implementation tracking, and preparing risk-informed recommendations for management review.

6.1.4 Contractor shall support the management, tracking, analysis, and reporting of Plans of Action and Milestones ("POA&Ms"), risk acceptances, and related remediation activities. Contractor shall coordinate with applicable stakeholders to document findings, track remediation progress, monitor due dates and milestone dates, collect and validate closure evidence, and provide status reporting on open, overdue, closed, and risk-accepted items. Contractor shall identify trends and recurring issues and provide recommendations for process improvement and risk reduction.

6.1.5 Contractor shall provide vulnerability management support as a sustained enterprise function. This support shall include vulnerability tracking, analysis, reporting, remediation coordination, and trend analysis across systems, applications, devices, and other in-scope assets. Contractor shall support the identification, documentation, prioritization, monitoring, and closure of vulnerabilities and shall assist stakeholders in evaluating remediation actions, timelines, and residual risk.

6.1.6 Contractor shall perform analysis of vulnerability data, scan results, remediation status, and related security findings to facilitate risk-based decision making. Contractor shall support meetings with applicable stakeholders to review vulnerability status, assist in remediation planning, identify aging vulnerabilities, and provide periodic reports that include severity, age, trend, and system-level status information.

6.1.7 Contractor shall lead, maintain, and track enterprise-wide configuration management activities as a dedicated, non-collateral security function. Contractor shall ensure that all systems within the authorization boundary are configured against approved security baselines (e.g., NIST, CIS) and that these baselines are continuously tuned and improved to reflect emerging threats and operational requirements.

6.1.7.1 Contractor shall be responsible for baseline development and maintenance by developing, documenting, and maintaining security configuration baselines for all enterprise assets (e.g., cloud, operating system, network, application). Baselines must be updated at least annually or upon significant changes to the environment to ensure alignment with current federal and organizational standards.

6.1.7.2 Contractor shall be responsible for active compliance monitoring and engineering by collaborating with the NOC/SOC and security engineering teams to utilize enterprise tools to perform automated configuration compliance scanning. Failed settings shall not remain static "tickets"; Contractor must analyze failures to determine if they represent a security risk, a technical conflict, or a requirement for a formal deviation.

6.1.7.3 Contractor shall be responsible for authorization boundary integration. The ISSO Lead and Security Engineers shall collaborate to ensure that all configuration data, including failed settings, technical deviations, and accepted risk decisions, are explicitly tracked and documented within the system's authorization boundary (e.g., Xacta/GRC tool).

6.1.7.4 Contractor shall be responsible for deviation and risk decision management by managing the full lifecycle of configuration deviations. This includes performing Security Impact Analyses (SIA) for requested deviations, facilitating the risk acceptance process with the CISO/ISSM, and ensuring that all approved deviations are reviewed annually for continued necessity.

6.1.7.5 Contractor shall support continuous tuning and improvement by implementing a "maintenance cycle" for configurations, tuning detection rules and settings to reduce "noise" while increasing the overall defensive posture.

6.1.8 Contractor shall support continuous monitoring and compliance activities intended to maintain awareness of the effectiveness of security controls over time. This support shall include reviewing compliance-related activities, identifying gaps, assisting with documentation updates, coordinating with system and business stakeholders, and

supporting the maturation of ongoing monitoring processes. Contractor shall support the maintenance of procedures and repeatable processes that improve visibility into the security and compliance posture of the enterprise.

6.1.9 Contractor shall support risk management activities associated with enterprise cybersecurity operations, including risk identification, risk analysis, risk tracking, and mitigation support. Contractor shall provide risk-informed recommendations related to vulnerabilities, control gaps, system changes, authorization issues, third-party risks, and other security matters that may affect the confidentiality, integrity, or availability of organizational systems and information.

6.1.10 Contractor shall serve as the primary technical support for all internal and external audits and assessments (e.g., annual FCC OIG FISMA audit, system assessments, internal audits). Contractor shall drive artifact collection by providing comprehensive documentation and investigation artifacts (e.g., logs, system configurations, access lists) required for compliance requests. Contractor shall provide liaison support by participating in accreditation interviews and audit meetings to provide technical insight into incident response and monitoring activities. Contractor shall perform evidence validation by ensuring all provided artifacts are complete, accurate, and of sufficient quality to support official oversight.

6.1.11 Contractor shall manage the Information Security Continuous Monitoring (ISCM) program and perform internal controls testing to ensure the persistent authorization and compliance of all enterprise systems. Key responsibilities include the proactive maintenance and update of A&A packages, including System Security Plans (SSPs), Configuration Management Plans (CMPs), and Contingency Plans, to ensure they remain accurate and conform to NIST SP 800-18 and USAC standards. Contractor shall serve as a liaison between business units and OCISO, facilitating weekly security meetings and managing inquiries related to system modifications, implementation initiatives, or problem resolution. Contractor shall perform annual policy and procedure gap analyses to ensure alignment with federal requirements. To verify that security controls remain effective over time, Contractor shall conduct routine reviews of audit logs, patching status, access lists, and incident response testing. As directed, Contractor shall execute internal Security Control Assessments (SCA) and controls testing for minor systems, interim authorizations, or FedRAMP SaaS offerings using NIST SP 800-53A as a guide.

6.1.12 Contractor shall support Supply Chain Risk Management (SCRM) activities under this task area to the extent such activities are part of the organization's broader risk and compliance framework, including coordination with stakeholders, maintenance of SCRM-related records, and development of risk mitigation recommendations.

6.1.13 Contractor shall provide support for cybersecurity training and awareness activities that are directly related to compliance responsibilities, role-based security obligations, and privileged or specialized security functions.

6.1.14 Contractor shall provide support for Supply Chain Risk Management (SCRM), implementation of AI security capabilities, and emerging cybersecurity capabilities to assist the organization in evaluating, managing, and improving its security posture with respect to third-party technologies, evolving cyber risks, and new operational capabilities.

6.1.15 Contractor shall support the operation and enhancement of the organization's SCRM activities, including documentation support, stakeholder coordination, maintenance of records, analysis of third-party and technology-related security risks, and preparation of risk mitigation recommendations. Contractor shall support the identification of gaps in current SCRM practices and provide recommendations for process improvement, monitoring, governance, and reporting.

6.1.16 Contractor shall support AI security-related compliance, vulnerability, and risk activities associated with software, systems, services, tools, or services that incorporate AI-enabled functions or emerging technologies that may affect enterprise risk. Such support may include security review support, risk analysis, recommendations for secure implementation, support for governance considerations, and coordination with stakeholders regarding the security implications of emerging technical capabilities.

6.2 Task Area 2: Integrated 24x7x365 Security Operations Center and Network Operations Center Support

6.2.1 Contractor shall provide integrated 24x7x365 Security Operations Center (SOC) and Network Operations Center (NOC) support to monitor, analyze, triage, escalate, coordinate, and report on cybersecurity and network events affecting enterprise systems, services, and infrastructure. Contractor shall maintain an operational support capability that provides continuous awareness of security events, network conditions, operational anomalies, incidents, outages, and other conditions requiring action or escalation.

6.2.2 Contractor shall continuously monitor enterprise security and network telemetry, alerts, status indicators, event feeds, case queues, and other operational sources to identify potential cybersecurity incidents, suspicious activity, performance anomalies, network disruptions, or other conditions requiring triage, investigation, coordination, or escalation. Contractor shall document and track such events using approved processes and maintain awareness of current and ongoing operational activity across the enterprise.

6.2.3 Contractor shall perform event intake, triage, initial analysis, and escalation for cybersecurity and network events in accordance with defined priorities, service levels, and standard operating procedures. Contractor shall gather relevant information, assess operational significance, route tickets or cases to the appropriate personnel or

stakeholders, and support incident coordination through closure or handoff, as applicable.

6.2.4 Contractor shall provide coordinated support for cybersecurity incident intake and response activities, including the receipt and processing of internally generated, externally reported, or user-reported security events and incidents. Contractor shall support incident communications, track actions taken, document findings, and coordinate with other organizational stakeholders as necessary to ensure timely response and situational awareness.

6.2.5 Contractor shall provide network monitoring support necessary to identify outages, degradations, anomalous behaviors, and other network-related operational conditions. Contractor shall support event correlation between cyber and network operations as necessary to improve situational awareness, reduce response delays, and improve the identification of root causes or interdependencies affecting enterprise operations.

6.2.6 Contractor shall perform a technical and procedural review of every incident and high-priority event to improve the enterprise security posture. Contractor shall support gap identification by analyzing security events to identify gaps in existing controls, visibility, or response procedures. Contractor shall conduct Root Cause Analyses (RCA) to determine the root cause of security and network anomalies to prevent recurrence. Contractor shall provide posture recommendations through actionable recommendations to improve detection, prevention, and response capabilities based on real-world event data.

6.2.7 Contractor shall execute hypothesis-driven threat hunting to identify abnormal behavior that evades automated detections. Contractor shall conduct daily proactive threat hunting within all SIEMs and other telemetry sources to identify suspicious patterns based on active vulnerability reports, threat reports, intelligence feeds, etc. Contractor shall maintain continuous coordination through frequent communication with the Security Operations staff to understand emerging threats and prioritize hunting efforts. Contractor shall document all hunting investigations in Splunk or another approved mechanism; high-risk findings must be escalated immediately. To ensure effective knowledge transfer, Contractor shall ensure every closed investigation or ticket has an associated Knowledge Base (KB) article created or linked within five (5) business days.

6.2.8 Contractor shall support operational communications and reporting, including shift turnover information, incident and event status updates, dashboard updates, operational summaries, and coordination with designated stakeholders. Contractor shall maintain sufficient records and documentation to support continuity of operations, knowledge sharing, service oversight, and performance measurement.

6.2.9 Contractor shall lead the enterprise in maintaining IR readiness through structured training and simulation. Contractor shall conduct exercise planning by developing an annual Incident Response Tabletop Exercise (TTX) plan in coordination with the

Privacy team and other IT stakeholders. Contractor shall conduct scenario development by designing at least three (3) distinct, high-fidelity scenarios per exercise, incorporating both cybersecurity (e.g., ransomware) and privacy-related (e.g., PII breach) components. Contractor shall facilitate and execute the annual TTX with participation from relevant departments, ensuring all communication and incident handling procedures are tested for efficiency.

6.2.10 Contractor shall create, maintain, and update standard operational procedures (SOP), playbooks, and general knowledge materials via the approved KB related to SOC/NOC operations, incident and event handling, escalation, and reporting. Contractor shall support the continuous improvement of operational processes to improve efficiency, consistency, and quality of service delivery.

6.3 Task Area 3: Security Engineering, SIEM, and Enterprise Monitoring Support

6.3.1 Contractor shall provide security engineering, SIEM, and enterprise monitoring support necessary to maintain, improve, and expand the technical capabilities that support cybersecurity monitoring, alerting, data analysis, and operational visibility. Contractor shall provide technical engineering support for monitoring platforms, telemetry sources, data integrations, and supporting security architecture functions required to sustain effective enterprise monitoring services.

6.3.2 Contractor shall support the administration, configuration, sustainment, enhancement, and optimization of SIEM-related capabilities and associated monitoring functions. This support shall include onboarding and integrating new data sources, normalizing and validating telemetry, improving visibility coverage, tuning alerts and rules, supporting correlation logic, and enhancing the usefulness of monitoring outputs for operational teams.

6.3.3 Contractor shall provide engineering support for enterprise monitoring capabilities, including support for log management, data handling, alert tuning, detection optimization, and operational analytics improvements. Contractor shall identify gaps in visibility, data coverage, or monitoring capability and provide recommendations for corrective actions and service improvements.

6.3.4 Contractor shall support the development, maintenance, and improvement of monitoring-related procedures, technical documentation, engineering baselines, and implementation guidance necessary to sustain enterprise cybersecurity monitoring functions. Contractor shall work with relevant stakeholders to improve monitoring coverage, increase the reliability of operational outputs, and support enterprise security objectives through engineering and technical analysis.

6.3.5 Contractor shall ensure that all security tools and detections remain effective and "high-signal" through ongoing refinement. Contractor shall conduct detection refinement in coordination with the NOC/SOC to regularly tune SIEM rules, EDR alerts, WAF/CDN,

etc., policies to reduce false positives and improve detection accuracy. Contractor shall conduct data validation by continuously normalizing and validating telemetry from existing and new data sources (e.g., Zscaler Secure Access Service Edge (SASE), Microsoft Defender). Contractor shall support configuration management efforts by monitoring and reporting on the effectiveness of security controls over time in collaboration with the NOC/SOC, identifying and correcting configuration drift.

6.4 Task Area 4: Security Architecture and Emerging Cybersecurity Capabilities

6.4.1 Contractor shall support the development and implementation of a robust and mature Security Architecture capability

6.4.2 Contractor shall establish and operationalize Security Architecture as a mature and robust enterprise function to ensure all systems are designed with a "security-by-design" and Zero Trust mindset.

6.4.3 Operationalizing Security Architecture:

6.4.3.1 Maturity Development: Contractor shall define and execute a Security Architecture maturity roadmap, including the adoption and implementation of the USAC selected Cybersecurity Reference Model that best fits the USAC Information Security Program, moving from a reactive review function to a strategic advisory capability that predicts threats and measures real-time architectural risks.

6.4.3.2 Architectural Evaluation: Contractor shall conduct cybersecurity-focused reviews of existing and proposed enterprise architectures, identifying technical debt and misalignments with NIST 800-207, NIST CSF 2.0, USAC Zero Trust Architecture Roadmap, and other relevant best practice reference guidance / guidelines.

6.4.3.3 Standards and Baselines: Contractor shall develop hardened architecture patterns and engineering baselines for cloud, on-premises, and hybrid environments.

6.4.4 Zero Trust Architecture (ZTA) Planning and Implementation:

6.4.4.1 Phase 1 Execution (Implementation/Operationalization): Contractor shall complete the rollout and operationalization of the Microsoft 365 security suite, including, but not limited to:

6.4.4.1.1 Microsoft Intune: Device health reporting and unified endpoint management.

6.4.4.1.2 Defender for Endpoint: EDR deployment and XDR integration.

6.4.4.1.3 Microsoft Purview: Implementation of DLP and sensitive data risk assessments.

6.4.4.1.4 Mobile Access: Secure mobile connectivity via ZTNA and Intune Mobile Application Management (MAM).

6.4.4.1.5 Privileged Access Management: Planning and implementation of Privileged Access Management (PAM) mechanisms utilizing established and in-place platforms (including but limited to CyberArk, Microsoft Entra Privileged Identity Management [PIM], Okta).

6.4.4.2 Phase 1 Planning (Remainder): Contractor shall develop technical requirements, implementation plans, and execute the necessary cybersecurity areas including, but not limited to:

6.4.4.2.1 Defender for Servers & Cloud Apps (CASB): Integration of server-side telemetry and SaaS security.

6.4.4.2.2 SASE: Migration from traditional VPNs to a SASE model.

6.4.4.2.3 Security Orchestration, Automation, and Response (SOAR) & Conditional Access: Engineering automated response playbooks and identity-centric access policies.

6.4.4.3 Phase 2 Objectives (Enhanced Process & Workflow):

6.4.4.3.1 Contractor shall define the transformation strategy for Conditional Access across all platforms, ensuring continuous verification of user identity and device health for every session.

6.4.4.3.2 Once the goals and strategy for Phase 2 is accepted and approved by USAC, Contractor shall lead the planning for and implementation of Phase 2 objectives.

6.4.4.4 Phase 3 Objectives (Programmatic/App Dev):

6.4.4.4.1 Contractor shall establish long-term goals for integrating security into application delivery pipelines, focusing on automated maintenance and programmatic security guardrails.

6.4.4.4.2 Once the goals and strategy for Phase 3 is accepted and approved by USAC, Contractor shall lead the planning for and implementation of Phase 2 objectives.

6.4.5 Emerging Capabilities & Automation: Contractor shall support the identification and evaluation of opportunities to improve cybersecurity capabilities through modernization, automation, analytics, or emerging techniques, provided such support is within scope and approved by the organization. Contractor shall provide recommendations in a manner that supports secure adoption, governance, and operational effectiveness.

6.4.5.1 Drive Automation and Prevention: Contractor shall evaluate and implement emerging tools, as designated by USAC, that utilize AIOps and behavioral analytics to automate incident containment and prevent attacks before they manifest.

6.4.5.2 Predictive Analytics: Support the adoption of machine learning-based security analytics to identify patterns indicative of advanced persistent threats (APTs).

6.5 Task Area 5: Program Management, Reporting, Performance Management, and Transition Support

6.5.1 Contractor shall provide overall program management, reporting, performance management, and transition support necessary to ensure disciplined execution of all requirements under this Section B: Statement of Work. Contractor shall provide management controls, staffing oversight, quality management, communications support, reporting cadence, and performance measurement mechanisms needed to support transparent and effective service delivery.

6.5.2 Contractor shall provide program management support to include planning, coordination, staffing oversight, quality control, risk and issue management, communications support, meeting support, and maintenance of management artifacts necessary to direct and oversee performance under this Section B: Statement of Work. Contractor shall maintain a structured management approach that supports accountability, quality, continuity, and timely delivery of required services and deliverables.

6.5.3 Contractor shall provide recurring reports, briefings, dashboards, metrics, and performance summaries in accordance with the deliverables and reporting cadence established under this Section B: Statement of Work. Reporting shall support operational awareness, management oversight, executive visibility, and the review of service levels, KPIs, vulnerabilities, risks, incidents, staffing, and service improvements.

6.5.4 Contractor shall establish and maintain a performance management process that supports the tracking, measurement, and review of service performance, including Service Level Agreements (SLAs), Key Performance Indicators (KPIs), and other contract performance measures. Contractor shall identify performance issues, support corrective action planning, and recommend service improvements as necessary to maintain acceptable performance.

6.5.5 As tasked, Contractor shall facilitate the transition of contracted activities and services to organization personnel or to a follow-on contractor at the beginning or at the end of the contract period of performance. Representative activities under this task area may include: providing current versions of all system and user documentation; providing all licensing and renewal information, asset management records, software documentation, and training materials; providing a current inventory of all organization-owned assets used by Contractor along with full support in the reconciliation of this inventory; providing current versions of all operational

procedures, standard operating procedures, guidelines, performance reports, specifications for hardware and software, in-flight activities, and other pertinent information needed to continue the services being performed by Contractor; and providing shadowing and other knowledge transfer meetings and opportunities to facilitate the transfer of information, processes, and data needed to continue the services being performed by Contractor.

7. DELIVERABLES

Contractor shall prepare, maintain, and submit all deliverables required under this Section B: Statement of Work in accordance with the timelines, formats, and review procedures established by the organization. Deliverables shall be complete, accurate, current, and of sufficient quality to support operational oversight, performance management, risk management, continuity of operations, and transition support.

All deliverables shall be submitted in an organization-approved electronic format unless otherwise directed. Contractor shall update recurring deliverables as required to reflect current operational conditions, staffing, risks, metrics, and service performance. Where a deliverable is described as a living document, Contractor shall maintain the deliverable throughout the period of performance and document material changes in the applicable recurring status report.

Table 1. Deliverables Summary

Section Ref. / Deliverable No.	Deliverable Title	Submission Frequency	Purpose / Contents
7.1.1	Transition-In Plan	One-time, NLT 7 days after contract award	Approach for assumption of services, onboarding, knowledge transfer, milestones, dependencies, and transition risk mitigation, based on review of the incumbent's Transition-Out Plan and coordination with the OCISO.
7.1.2	Transition-In Support Package	One-time, NLT 45 days after contract award	Documentation, inventories, licensing, procedures, in-flight activities, and knowledge transfer materials needed to maintain continuity of services.
7.1.3	Program Management Plan	Initial submission; updated as needed	Management approach, reporting structure, communications, quality approach, staffing oversight, and risk/issue management.
7.1.4	Staffing Plan	Initial submission; updated as needed	Labor categories, coverage model, qualifications, certifications, continuity approach, and surge/backup strategy.

Section Ref. / Deliverable No.	Deliverable Title	Submission Frequency	Purpose / Contents
7.1.5	Quality Control Plan	Initial submission; updated as needed	Methods and controls used to ensure quality, consistency, timeliness, accuracy, and corrective action management.
7.1.6	Transition-Out Plan	One-time, NLT 90 days before contract expiration	Approach for turnover of services, documentation, assets, knowledge, and responsibilities to organization personnel or follow-on contractor.
7.1.7	Transition-Out Support Package	One-time, NLT 60 days before contract expiration	Documentation, inventories, licensing, procedures, in-flight activities, and knowledge transfer materials needed to maintain continuity of services.
7.2.1	Bi-Weekly Planning Report	Bi-weekly	Summary of (1) work performed in prior 2-week period; (2) major activities, issues, risks, staffing updates, and operational developments impacting work; and (3) planned work for next 2-week period with highlighted impacts.
7.2.2	Monthly Status Report	Monthly	Comprehensive summary of key accomplishments, open issues, risks, staffing changes, service performance highlights, and next-period activities, per contractual requirements and in support of monthly invoice.
7.2.3	Weekly Operational Summary	Weekly	Summary of SOC/NOC activity, notable events, alert and ticket volumes, incident coordination, and significant outages or issues.
7.2.4	Meeting Minutes and Briefing Materials	As directed / recurring meetings	Agendas, minutes, briefing slides, and action-item summaries for management, operational, and coordination meetings.
7.2.5	Weekly ZTA Phase 1 Operational Status Report	Weekly	Progress report on Intune, Defender for Endpoint, Purview, Mobile Access, and PAM rollout.
7.2.6	Monthly Phase 2 Strategic Roadmap	Monthly	Refine and update the roadmap for ZTA Phase 2 based on objectives for workflow-level Zero Trust.

Section Ref. / Deliverable No.	Deliverable Title	Submission Frequency	Purpose / Contents
7.2.7	Monthly Phase 3 Strategic Roadmap	Monthly	Refine and update the roadmap for ZTA Phase 3 based on objectives for application-level Zero Trust.
7.2.8	Periodic Security Architecture Review Findings	Periodic	Provide evaluation results for new or updated enterprise systems.
7.2.9	Monthly Tool Tuning & Optimization Log	Monthly	Record of all detection rule updates and policy refinements.
7.3.1	Security Compliance Status Report	Periodic	Status of compliance activities, authorization-related actions, documentation updates, control monitoring, and improvement recommendations.
7.3.2	Annual Enterprise Configuration Management Plan (CMP)	Annual	A comprehensive document outlining the strategy, roles, and automated tools used for CM across the authorization boundary.
7.3.3	Monthly Configuration Compliance and Deviation Report	Monthly	A high-level summary of compliance percentages, open deviations, and a list of failed settings currently being tracked to the authorization boundary.
7.3.4	Quarterly Security Baseline Tuning and Optimization Log	Quarterly	Documentation of updates made to baseline settings, including the rationale for changes and the results of the “tuning” cycle.
7.3.5	Security Impact Analysis (SIA)	As directed	Formal assessment of the risk introduced by a system change or configuration deviation, provided to the ISSM/CISO for approval.

Section Ref. / Deliverable No.	Deliverable Title	Submission Frequency	Purpose / Contents
7.3.6	Configuration Management Risk and Decision Register	Ongoing	Real-time tracking of all risk-accepted configuration settings within the approved system of record.
7.3.7	A&A Packages Per System	Annually; otherwise as needed according to outcome of SIA	Comprehensive updates to system security, configuration, and contingency documentation.
7.3.8	Annual Policy and Procedure Gap Review	Annually	Review and identify compliance gaps in current policies and procedures.
7.3.9	Internal Controls Testing / SCA Report	Annually	Support USAC staff to conduct internal controls testing and provide documentation of results for internal assessments of systems as designated and approved by the CISO for certain minor systems, interim authorizations, or SaaS offerings.
7.3.10	Control Effectiveness Review Report	Quarterly	Conduct a quarterly review of each system and provide a summary of routine checks on logs, access lists, account maintenance, and configuration status.
7.3.11	Audit Artifact Package	Periodic	Compile documentation and evidence for specific audit cycles.
7.3.12	Weekly Audit Status Report	Weekly	Summary of artifact requests, meeting outcomes, and potential findings during active audits.
7.3.13	POA&M Status Report	Periodic	Status of open, closed, overdue, and risk-accepted items, milestone progress, aging trends, and items requiring management attention.
7.3.14	Vulnerability Management Report	Periodic	Vulnerability trends, severity, age, remediation progress, unresolved issues, and recommendations.
7.3.15	SCRM Status Report	Periodic	Summary of supply chain risk activities, identified issues, mitigation recommendations, and program/process updates.

Section Ref. / Deliverable No.	Deliverable Title	Submission Frequency	Purpose / Contents
7.4.1	KPI / SLA Dashboard	Ongoing	Maintenance of a management-ready dashboard with available performance measures, service levels, response trends, vulnerability trends, and reporting timeliness, subject to refinement at direction of the CISO.
7.4.2	Quarterly Performance Review Briefing	Quarterly	Summary of service performance, key trends, risks, accomplishments, improvement areas, and recommendations.
7.4.3	Annual Lessons Learned Report	Annually	Summary of significant observations, recurring issues, improvement opportunities, and recommendations for service enhancement.
7.5.1	Incident Report / After Action Report	As directed	Documentation of major incidents, operational impacts, actions taken, lessons learned, and recommended follow-up actions.
7.5.2	Monthly Security Control Gap and Recommendation Report	Monthly	Summary of recommended actions needed as result of documented events and/or incidents.
7.5.3	Daily Threat Hunting Logs	Daily	Records of proactive investigations performed within the SIEM or other telemetry source(s).
7.5.4	Bi-Weekly Threat Activity Report	Bi-weekly	Summary of investigations, findings, and recommendations for staff.
7.5.5	Standard Operating Procedures (SOP), Playbooks, and Knowledge Base (KB) Maintenance	Ongoing	Creation of new, and maintenance of existing, SOPs, Playbooks, and KB, as driven by need and changing conditions impacting the guidance information, subject to review and direction of the OCISO.

Section Ref. / Deliverable No.	Deliverable Title	Submission Frequency	Purpose / Contents
7.5.6	Annual Tabletop (TTX) Scenario Plan	Annually	Detailed outline of TTX exercise goals and scenarios.
7.5.7	Annual Tabletop (TTX) After Action Report	Annually	Formal summary of the TTX exercise, including observations and recommendations for IR improvement, delivered within ten (10) business days of TTX conclusion.

7.1 Transition and Program Management Deliverables

7.1.1 Transition-In Plan: To be delivered for approval no later than seven (7) days after contract award, Contractor shall provide a Transition-In Plan that describes the approach for assuming responsibility for in-scope services, onboarding personnel, coordinating knowledge transfer, establishing operational readiness, and minimizing disruption to ongoing services. The plan shall include key milestones, responsibilities, dependencies, and risk mitigation strategies associated with transition activities.

7.1.2 Transition-In Support Package: To be delivered no later than forty five (45) days after contract award, Contractor shall provide a Transition-In Support Package demonstrating knowledge and understanding of the enterprise provide relevant to the tasks and deliverables contained in this Section B: Statement of Work that includes, but is not limited to, current system and user documentation, licensing and renewal information, asset management records, software documentation, training materials, current inventories of organization-owned assets used by Contractor, current operational procedures, standard operating procedures, guidelines, performance reports, hardware and software specifications, in-flight activities, and other relevant materials required to continue performance of the services. Contractor shall also support shadowing sessions, knowledge transfer sessions, and other transition support activities necessary to facilitate continuity of operations.

7.1.3 Program Management Plan: Contractor shall provide a Program Management Plan describing the management approach, reporting structure, communications methods, quality approach, staffing oversight, risk and issue management approach, and overall method for performing the requirements of this Section B: Statement of Work. This plan shall be maintained throughout performance and updated as necessary to reflect approved changes.

7.1.4 **Staffing Plan:** Contractor shall provide a Staffing Plan that identifies proposed labor categories, staffing approach, coverage model, qualifications, certifications, continuity approach, and surge or backup support strategy necessary to perform the requirements of this Section B: Statement of Work. The Staffing Plan shall support continuous operations and demonstrate Contractor's ability to maintain adequate staffing throughout the period of performance.

7.1.5 **Quality Control Plan:** Contractor shall provide a Quality Control Plan describing the methods, procedures, and controls used to ensure quality, consistency, timeliness, and accuracy in the performance of all services and deliverables under this Section B: Statement of Work. The plan shall include methods for identifying performance deficiencies, implementing corrective actions, and preventing recurrence.

7.1.6 **Transition-Out Plan:** To be delivered for approval no later than ninety (90) days before contract expiration, Contractor shall provide a Transition-Out Plan describing the approach for transitioning services, documentation, assets, knowledge, and responsibilities to organization personnel or a follow-on contractor. The plan shall include milestones, responsibilities, transition support activities, continuity measures, and knowledge transfer methods.

7.1.7 **Transition-Out Support Package:** To be delivered no later than sixty (60) days before contract expiration, Contractor shall provide a Transition-Out Support Package that demonstrates knowledge and understanding of the enterprise that includes, but is not limited to, current system and user documentation, licensing and renewal information, asset management records, software documentation, training materials, current inventories of organization-owned assets used by Contractor, current operational procedures, standard operating procedures, guidelines, performance reports, hardware and software specifications, in-flight activities, and other relevant materials required to continue performance of the services. Contractor shall also support shadowing sessions, knowledge transfer sessions, and other transition support activities necessary to facilitate continuity of operations.

7.2 Operational Reporting Deliverables

7.2.1 **Bi-Weekly Planning Report:** Contractor shall provide a Bi-Weekly Planning Report that will (1) summarize work performed to the current plan in the previous two-week period; (2) identify major activities, issues, risks, staffing updates, and operational developments impacting planned work; and (3) summarize work planned for the following two-week period highlight changes, delays, risks, and issues impeding or impacting the planned work.

7.2.2 **Monthly Status Report:** Contractor shall provide a Monthly Status Report that comprehensively summarizes activities performed during the reporting period, key accomplishments, open issues, risks, staffing changes, service performance highlights,

and planned activities for the upcoming period. The report shall include updates to living management documents, as applicable. This deliverable shall support the monthly invoice per contract.

7.2.3 Weekly Operational Summary: Contractor shall provide a Weekly Operational Summary that includes a summary of SOC/NOC operational activity, notable events, alert and ticket volumes, major incident coordination activities, significant outages or operational issues, and other operationally relevant information.

7.2.4 Meeting Minutes and Briefing Materials: Contractor shall prepare and submit meeting agendas, meeting minutes, presentation materials, and action item summaries for recurring management, operational, audit, and coordination meetings as directed.

7.2.5 Weekly ZTA Phase 1 Operational Status Report: Contractor shall provide a progress report on Intune, Defender for Endpoint, Purview, Mobile Access, and PAM rollout.

7.2.6 Monthly Phase 2 Strategic Roadmap: Contractor shall refine and update the roadmap for ZTA Phase 2 based on objectives for workflow-level Zero Trust.

7.2.7 Monthly Phase 3 Strategic Roadmap: Contractor shall refine and update the roadmap for ZTA Phase 3 based on objectives for application-level Zero Trust.

7.2.8 Periodic Security Architecture Review Findings: Contractor shall provide evaluation results for new or updated enterprise systems.

7.2.9 Monthly Tool Tuning & Optimization Log: Contractor shall provide a record of all detection rule updates and policy refinements, including, but not limited to, detection refinement, data validation, and configuration management.

7.3 Compliance, Risk, and Vulnerability Deliverables

7.3.1 Security Compliance Status Report: Contractor shall provide a periodic Security Compliance Status Report summarizing the status of compliance activities, authorization-related actions, documentation updates, control monitoring activities, outstanding issues, and recommendations for improvement.

7.3.2 Annual Enterprise Configuration Management Plan (CMP): Contractor shall develop a comprehensive document outlining the strategy, roles, and automated tools used for CM across all authorization boundaries.

7.3.3 Monthly Configuration Compliance and Deviation Report: Contractor shall develop a high-level summary of compliance percentages, open deviations, and a list of failed settings currently being tracked against each authorization boundary.

7.3.4 Quarterly Security Baseline Tuning & Optimization Log: Contractor shall provide documentation of updates made to baseline settings, including the rationale for changes and the results of the “tuning” cycle.

7.3.5 Security Impact Analysis (SIA): Contractor shall provide a formal assessment of the risk introduced by a systems change and/or configuration deviation provided to the ISSM/CISO for approval.

7.3.6 Configuration Management Risk and Decision Register: Contractor shall track all rick-accepted configuration settings within the approved system of record.

7.3.7 A&A Packages Per System: Contractor shall provide comprehensive updates to system security, configuration, and contingency documentation following NIST guidelines at least annually or upon approved changes necessitating an update to the package.

7.3.8 Annual Policy and Procedure Gap Review: Contractor shall review and identify compliance gaps in current policies and procedures. The Contract shall make recommendations for improvements to policies and procedures to improve compliance and operational integrity.

7.3.9 Internal Controls Testing / SCA Report: As directed, Contractor shall support USAC staff to conduct internal controls testing and provide documentation of results for internal assessments of systems as designated and approved by the CISO for certain minor systems, interim authorizations, or SaaS offerings that do not require formal, third-party assessment.

7.3.10 Control Effectiveness Review Report: Contractor shall conduct a quarterly review of each system and provide a summary of routine checks on logs, access lists, account maintenance, and configuration status.

7.3.11 Audit Artifact Package: Contractor shall compile documentation and evidence for specific audit cycles (e.g., annual FCC OIG FISMA audit, system assessment, internal audits). Contractor shall serve as the primary POC and liaison with the appropriate audit personnel (e.g., FCC OIG, assessor, internal auditor) unless otherwise directed.

7.3.12 Weekly Audit Status Report: Contractor shall provide a summary of artifact requests, meeting outcomes, recommended actions, and potential observations/findings during active audits.

7.3.13 POA&M Status Report: Contractor shall provide a POA&M Status Report that includes open, closed, overdue, and risk-accepted items; milestone status; aging trends; and issues requiring management attention.

7.3.14 Vulnerability Management Report: Contractor shall provide a Vulnerability Management Report summarizing vulnerability status, trends, severity, age, remediation progress, unresolved issues, and recommendations.

7.3.15 SCRM Status Report: Contractor shall provide a periodic SCRM Status Report summarizing supply chain risk support activities, identified issues, risk observations, mitigation recommendations, and program or process updates.

7.4 Performance Metrics and Dashboard Deliverables

7.4.1 KPI / SLA Dashboard: Contractor shall provide a recurring KPI / SLA Dashboard that presents contract performance measures in a clear, management-ready format. At a minimum, the dashboard shall include service levels, trends, response or triage measures, vulnerability or remediation trends, reporting timeliness, and other performance indicators defined under this Section B: Statement of Work.

7.4.2 Quarterly Performance Review Briefing: Contractor shall provide a Quarterly Performance Review Briefing summarizing service performance, key trends, risks, major accomplishments, areas for improvement, and recommendations for service enhancement.

7.4.3 Annual Lessons Learned Report: Contractor shall provide an Annual Lessons Learned Report documenting significant observations, recurring issues, improvement opportunities, performance insights, and recommendations for future service enhancements.

7.5 Incident Response and NOC/SOC Support Deliverables

7.5.1 Incident Report / After Action Report: As directed, Contractor shall provide Incident Reports and After-Action Reports documenting major incidents, operational impacts, actions taken, coordination activities, lessons learned, and recommended follow-up actions.

7.5.2 Monthly Security Control Gap and Recommendation Report: Contractor shall develop a summary of recommended actions needed as result of documented events and/or incidents to improve IR, NOC, and/or SOC operations and/or general operational effectiveness across stakeholder teams.

7.5.3 Daily Threat Hunting Logs: Contractor shall provide records of proactive investigations performed within the SIEM or other telemetry source(s).

7.5.4 Bi-Weekly Threat Activity Report: Contractor shall develop a summary of investigations, findings, and recommendations for staff.

7.5.5 Standard Operating Procedures (SOP), Playbooks, Knowledge Base (KB) Maintenance: Contractor shall conduct periodic creation, maintenance, and updates to new and existing SOPs, Playbooks, and/or KB for the purpose of effective IR and NOC/SOC operations.

7.5.6 Annual Tabletop (TTX) Scenario Plan: Contractor shall develop a detailed outline of TTX exercise goals and scenarios. Contractor shall conduct the TTX after approval has been given for the Scenario Plan.

7.5.7 Annual Tabletop (TTX) After Action Report: Contractor shall deliver a formal summary of the TTX exercise, including observations and recommendations for IR improvement, delivered within ten (10) business days of TTX conclusion. The After-

Action Report will be used to identify improvement areas and/or actions for the NOC/SOC as well as other teams/components to be tracked as POA&Ms.

8. KEY PERSONNEL AND LABOR CATEGORIES

Contractor shall provide qualified personnel with the knowledge, skills, experience, and certifications necessary to perform all requirements under **Section B: Statement of Work**. Contractor shall maintain sufficient depth of staffing to ensure continuity of operations, including continuous support for 24x7x365 operational functions, management support, engineering activities, compliance support, and recurring deliverables.

Contractor shall propose and maintain labor categories aligned to the work described in this Section B: Statement of Work. Labor categories shall reflect functional responsibilities and support performance in the areas of compliance and risk support, SOC/NOC operations, security engineering, SIEM support, vulnerability management, SCRM, AI security, reporting, and program management.

8.1 Key Personnel

8.1.1 Program Manager: Contractor shall provide a Program Manager who shall serve as the primary point of contact for all programmatic matters under this Section B: Statement of Work. The Program Manager shall be responsible for overall contract performance, coordination, staffing oversight, risk and issue management, quality oversight, communications support, and management reporting.

8.1.2 Security Architect: Contractor shall provide a Security Architect responsible for establishing the Security Architecture capability and providing recommendations on the review and implementation of technology. This individual shall oversee the Security Architecture capability, drive the implementation of ZTA, and provide recommendations for the implementation of emerging cybersecurity technology.

8.1.3 SOC/NOC Operations Manager: Contractor shall provide a SOC/NOC Operations Manager responsible for oversight of integrated 24x7x365 security and network monitoring operations. This individual shall oversee operational workflows, escalation procedures, staffing coverage, shift coordination, event handling consistency, and operational reporting.

8.1.4 ISSO/ISCM Lead: Contractor shall provide an ISSO/ISCM Lead responsible for the strategic coordination of compliance, authorization support, and the comprehensive execution of the Information Security Continuous Monitoring (ISCM) program. This role leads the Risk Management Framework (RMF) and A&A lifecycle, ensuring that all security artifacts, including System Security Plans (SSP), Configuration Management Plans (CMP), and Disaster Recovery Plans (DRP), are continuously

maintained and updated to reflect the current operational environment. Beyond documentation oversight, the Lead facilitates proactive internal controls testing and internal Security Control Assessments (SCA) to verify that security controls remain effective over time. They act as the primary liaison between business functions and the Office of the CISO, coordinating weekly security meetings and managing the end-to-end lifecycle of POA&Ms, risk acceptances, and configuration deviations tracked directly to the system's authorization boundary. Additionally, this individual manages the collection of investigation artifacts for internal and external audits, such as FISMA and OIG, ensuring all evidence meets oversight quality standards.

8.1.5 Lead Cybersecurity Engineer: Contractor shall provide a Lead Security Engineer responsible for oversight of security engineering, SIEM support, monitoring architecture support, data source onboarding, alert tuning, and technical improvement activities related to enterprise monitoring.

8.1.6 Automation/SOAR Engineer: Contractor shall provide an Automation/SOAR engineer responsible for emerging capabilities and response automation. This individual shall be responsible for the configuration and implementation of emerging cybersecurity technologies, including, but not limited to, SOAR and/or automation platforms.

8.1.7 Lead PAM Engineer: Contractor shall provide a Lead PAM Engineer responsible for the planning and implementation of the PAM platform(s) across all systems, on-premises and cloud-based. This individual shall be responsible for stakeholder engagement, PAM architecture, and implementation.

8.1.8 Vulnerability Management Lead: Contractor shall provide a Vulnerability Management Lead responsible for coordination of vulnerability tracking, remediation support, reporting, trend analysis, and integration of vulnerability management activities into overall risk and compliance support.

8.2 Required Labor Categories

Contractor shall provide labor categories sufficient to perform all services required under this Section B: Statement of Work. At a minimum, Contractor shall provide personnel in labor categories substantially equivalent to the following:

- Program Manager
- Security Architect
- SOC/NOC Operations Manager
- ISSO Lead
- Lead Cybersecurity Engineer
- Vulnerability Management Lead
- Security Compliance / RMF Analyst
- SOC Analyst
- NOC Analyst
- Security Engineer / SIEM Engineer
- Automation / SOAR Engineer
- Lead PAM Engineer
- Vulnerability Management Analyst
- Threat Intelligence / Threat Hunting Analyst
- SCRM / Emerging Technology Security Analyst
- Reporting and Metrics Analyst
- Technical Writer / Documentation Specialist, as needed

8.3 Minimum Qualifications

Contractor shall ensure that proposed personnel possess education, certifications, training, and relevant experience appropriate to their assigned labor category. Personnel shall demonstrate experience performing similar work in enterprise cybersecurity, network operations, security engineering, security compliance, vulnerability management, or related environments of comparable scale, complexity, or criticality.

Key Personnel shall possess demonstrated experience leading or supporting enterprise-level cybersecurity service delivery, operational coordination, engineering support, or compliance support in complex environments.

8.4 Required Certifications

Contractor shall ensure Key Personnel hold certifications appropriate to their roles. Equivalent certifications may be accepted where they demonstrate substantially similar competency and are approved by the organization.

At a minimum, the following certifications are required:

- Program Manager: Project Management Professional (PMP), Certified Information Systems Security Professional (CISSP), and Certified Cloud Security Professional (CCSP), and/or relevant cybersecurity leadership competency certifications
- Security Architect: CISSP, Certified Information Security Manager (CISM), Systems Security Certified Practitioner (SSCP), and/or relevant cybersecurity architecture certifications
- SOC/NOC Operations Manager: CISSP and/or relevant incident response or security operations certification
- ISSO Lead: CISSP or equivalent information security governance/risk certification
- Lead Cybersecurity Engineer: CISSP, ISSEP, ITIL Foundation (latest revision), and/or equivalent advanced security engineering or architecture certification
- Lead PAM Engineer: CISSP, PMP, ISC2 Certified Information Systems Security Professional, and/or relevant platform certifications matching platform currently in use and targeted for future use
- Vulnerability Management Lead: relevant cybersecurity certification demonstrating competence in vulnerability management, risk, or operations support
- Operational and engineering staff: role-appropriate industry certifications in cybersecurity, network operations, systems security, or monitoring technologies, as applicable

8.5 Staffing Continuity and Substitution Requirements

Contractor shall maintain staffing continuity sufficient to ensure uninterrupted performance of all required services. Contractor shall provide backup coverage for Key Personnel and critical operational roles to account for leave, attrition, training, surge requirements, and other staffing disruptions.

Contractor shall notify the organization in advance of any proposed substitution of Key Personnel and shall provide the qualifications of any proposed replacement. Replacement personnel shall possess qualifications equal to or greater than those of the individual being replaced, unless otherwise approved.

Contractor shall ensure that staffing levels remain sufficient to support 24x7x365 operational requirements and all reporting, engineering, compliance, and transition-related obligations under this Section B: Statement of Work.

9. PERFORMANCE METRICS, SLAS, AND KPIS

Contractor shall perform all services under this Section B: Statement of Work in accordance with defined performance standards, Service Level Agreements ("SLAs"), and Key Performance Indicators ("KPIs") defined in IT Policies, Procedures, IT Security Standard Operating Procedures ("SOP") and deliverable definitions in this contract. Performance management shall be used to measure service quality, timeliness, operational effectiveness, responsiveness, and continuous improvement across all task areas.

Contractor shall establish and maintain a performance management approach that supports routine monitoring of service outcomes, trending of operational data, identification of deficiencies, and implementation of corrective actions where performance falls below required standards. Performance shall be reviewed through recurring reports, dashboards, meetings, and other management oversight mechanisms defined under this Section B: Statement of Work.

9.1 Performance Management Approach

Contractor shall develop, maintain, and execute a performance management process that measures performance across security compliance support, vulnerability management, integrated SOC/NOC operations, security engineering, SIEM and monitoring support, SCRM, AI security support, reporting, and transition activities. The performance management process shall support transparency, accountability, and service improvement throughout the period of performance.

Contractor shall provide performance data in a format suitable for operational oversight and executive review. Metrics shall be tracked over time to support trend analysis, service improvement planning, and early identification of operational, compliance, or staffing issues.

9.2 Service Level Agreements ("SLAs")

Contractor shall meet the service levels established by the organization for the performance of in-scope services. SLAs shall define expected service levels, the method of measurement, reporting frequency, and the responsibilities of Contractor for maintaining acceptable service performance.

At a minimum, SLAs may include, but are not limited to, the following service areas:

9.2.1 Event Triage and Response Timeliness: Contractor shall meet defined service levels for the acknowledgment, triage, escalation, and coordination of cybersecurity and network events. These measures shall apply to integrated SOC/NOC operations and may vary by priority or severity level.

9.2.2 Automation Efficacy: Contractor shall report on the percentage of incidents contained automatically without manual SOC intervention.

9.2.3 Vulnerability Management Timeliness: Contractor shall support tracking and coordination of vulnerability remediation activities in accordance with organization-

defined remediation timelines, severity prioritization, and risk-based thresholds. Vulnerability status shall be measured for timeliness, aging, trend, and closure support.

9.2.4 ZTA Implementation Milestone Adherence: Contractor shall support tracking and reporting on the percentage of Phase 1-3 tasks completed on schedule.

9.2.5 Architectural Compliance: Contractor shall report on the percentage of systems evaluated that meet defined hardening standards.

9.2.6 Reporting Timeliness: Contractor shall submit all recurring and event-driven deliverables on time and in the required format. Reporting timeliness shall be measured for all required reports, dashboards, incident reports, status reports, transition materials, and other deliverables identified in this Section B: Statement of Work.

9.2.7 Operational Coverage and Availability: Contractor shall maintain required staffing and service coverage necessary to support 24x7x365 SOC and NOC operations, as well as continuity of performance for management, compliance, engineering, and reporting functions.

9.2.8 Platform and Monitoring Support Availability: Contractor shall support the operational availability and sustainment of monitoring-related capabilities, engineering support functions, and SIEM-supporting services as defined by the organization.

A recommended starting point for operational triage service levels is as follows:

- Critical Priority Events: initial triage within one (1) hour
- High Priority Events: initial triage within six (6) hours
- Medium Priority Events: initial triage within twenty-four (24) hours
- Low Priority Events: initial triage within ten (10) business days or other organization-defined threshold

9.3 Key Performance Indicators ("KPIs")

Contractor shall track and report KPIs that measure the effectiveness, quality, and efficiency of services provided under this Section B: Statement of Work. KPIs shall be reviewed regularly and may be refined by the organization as operational needs mature.

9.3.1 Security Operations and Network Monitoring KPIs

- Mean Time to Detect (MTTD)
- Mean Time to Acknowledge
- Mean Time to Respond (MTTR)
- Mean Time to Contain
- Mean Time to Resolve
- Percentage of events triaged within SLA
- Number of events or incidents identified
- Number of incidents resolved or coordinated through closure
- False positive rate, where measurable
- Operational ticket or case backlog trends

9.3.2 Vulnerability Management KPIs

- Number of open vulnerabilities by severity
- Vulnerability aging by severity and system
- Number of vulnerabilities closed during reporting period
- Number of overdue vulnerabilities
- Percentage of vulnerabilities remediated within target timelines
- Trends in recurring or high-risk vulnerabilities

9.3.3 Compliance and Risk KPIs

- Number of open POA&Ms
- Number of overdue POA&Ms
- Number of POA&Ms closed during reporting period
- Number of risk acceptances or equivalent actions tracked
- Status of required compliance artifacts and documentation updates
- Percentage of recurring compliance activities completed on time

9.3.4 Configuration Management KPIs

- Approved Baseline Accuracy (assigned, approved security baseline for each system)
- Remediation/Decision Velocity (failed configuration settings remediated, risk-accepted, and assigned as POA&Ms within defined timeframes)
- Documentation Integrity (approved deviations have corresponding SIA and documented in approved system of record)

9.3.5 Engineering and Monitoring Support KPIs

- Number of data sources onboarded or updated
- Number of alert tuning or detection improvement actions completed
- Number of identified monitoring gaps and corrective actions initiated
- Time to implement approved monitoring changes
- Monitoring coverage trends, where measurable

9.3.6 Program Management and Reporting KPIs

- Percentage of deliverables submitted on time
- Percentage of required meetings supported on time
- Staffing continuity rate for key roles
- Number of open high-priority risks or issues
- Time to submit management reports and briefing materials
- Status of transition support activities, when applicable

9.3.7 SCRM and Emerging Capability KPIs

- Number of SCRM support actions completed
- Number of third-party or technology risk items reviewed
- Number of SCRM recommendations issued
- Number of AI security or emerging technology review actions completed
- Number of identified process improvements or modernization recommendations

9.4 Reporting Frequency and Performance Review

Contractor shall report performance data through the recurring reports and dashboards defined in Section 3 of this Section B: Statement of Work. At a minimum, performance data shall be reviewed through weekly operational summaries, bi-weekly and monthly status reports, quarterly performance review briefings, and annual lessons-learned reporting, as applicable.

Contractor shall participate in performance review meetings as directed and shall provide analysis of performance trends, issues affecting service levels, and recommended corrective or preventive actions when requested by the organization.

9.5 Corrective Action and Service Improvement

When performance falls below required thresholds, Contractor shall identify the cause of the deficiency, propose corrective actions, implement approved remediation steps, and report progress until the issue is resolved. Contractor shall also recommend service improvements where recurring trends, operational inefficiencies, control gaps, or engineering limitations affect performance.

10. APPLICABLE LAWS, DIRECTIVES, AND STANDARDS

Contractor shall perform all services under this Section B: Statement of Work in accordance with applicable statutes, regulations, executive directives, federal cybersecurity guidance, risk management requirements, and generally accepted industry best practices relevant to enterprise cybersecurity and network monitoring support services.

The references below are intended to provide the general legal, policy, and technical framework governing performance under this Section B: Statement of Work. The organization may update, supplement, or refine these references during performance to reflect changes in law, policy, or operational requirements.

10.1 Statutory and Regulatory Requirements

Contractor shall perform in accordance with applicable requirements and guidance, including, as applicable:

- Federal Information Security Modernization Act (FISMA)
- OMB Circular A-130, Managing Information as a Strategic Resource
- Other applicable federal privacy, records, and information protection requirements, as directed by the organization

10.2 Federal Cybersecurity Standards and Guidance

Contractor shall perform in accordance with applicable requirements and guidance, including, as applicable:

- Executive Order 14028, Improving the Nation's Cybersecurity
- NIST Cybersecurity Framework (CSF) 2.0
- NIST Special Publication (SP) 800-37, Risk Management Framework for Information Systems and Organizations
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations
- NIST SP 800-181, Workforce Framework for Cybersecurity (NICE Framework)
- NIST SP 800-218, Secure Software Development Framework (SSDF), where applicable

10.3 Risk Management, Continuous Monitoring, and Incident Response Standards

Contractor shall perform in accordance with applicable requirements and guidance, including, as applicable:

- NIST SP 800-61, Incident Response Recommendations and Considerations for Cybersecurity Risk Management
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-92, Guide to Computer Security Log Management
- OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents
- OMB M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response
- CISA Federal Government Cybersecurity Incident and Vulnerability Response Playbooks
- Other applicable incident response, vulnerability management, or monitoring guidance issued during the period of performance

10.4 Identity, Access, Zero Trust, and Cloud Security Standards

Contractor shall perform in accordance with applicable requirements and guidance, including, as applicable:

- OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
- NIST SP 800-63, Digital Identity Guidelines, as applicable
- FedRAMP requirements and guidance, where cloud services or cloud-based systems are in scope
- NIST and federal guidance relating to secure cloud architecture, identity, and privileged access management, as applicable

10.5 Supply Chain, Software Security, and Emerging Technology Guidance

Contractor shall perform in accordance with applicable requirements and guidance, including, as applicable:

- OMB M-21-30, Protecting Critical Software Through Enhanced Security Measures
- OMB M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices
- OMB M-23-16, Update to M-22-18 Enhancing Software Security
- NIST software supply chain security guidance
- Applicable federal guidance relating to supply chain risk management (SCRM), critical software, and secure adoption of emerging technologies
- Applicable USAC architectural guidance concerning AI-enabled systems, analytics, or automation, where such technologies are in scope
- NIST AI Risk Management Framework and Playbook as well as maintain currency with emerging standards and new publications from NIST on AI topics

10.6 Industry Standards and Best Practices

In addition to the federal references identified above, Contractor shall apply generally accepted industry standards and best practices appropriate to enterprise cybersecurity operations, vulnerability management, monitoring, engineering, and program management. Where conflicts arise between generally accepted practices and applicable laws, directives, or organizational requirements, the latter shall govern.

11. MEETINGS

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

Contractor shall schedule, coordinate, and hold a Contract "Kick-Off Meeting" (as described in this section and Section B.8) no later than ten (10) workdays after any Contract award, at USAC Headquarters or virtually as approved by USAC. The Kick-Off Meeting will provide an introduction between Contractor Staff and USAC personnel who will be involved with the awarded Contract. The meeting will provide the opportunity to discuss technical, management, and security issues, and review Contractor's proposed project timeline and reporting procedures. At a minimum, the attendees shall include Key Personnel (as described in Section C.1.N), Contractor Staff capable of obligating Contractor, and USAC personnel.

Meetings that involve or contain disclosure of: (a) program participants' PII, (b) confidential information, or (c) contribution data, cannot be recorded. If Contractor needs to record a meeting, such as project kick-off, status update, etc., Contractor must use the teleconferencing software's native recording functionality and obtain USAC's approval prior to any recording. If approved, Contractor must indicate the meeting will be recorded in the meeting invite and verbally mention in the meeting, as well as provide the recording to the appropriate USAC point of contact, within one week in compliance with USAC's Audio and Video Meeting Recording Policy.

12. TRAVEL

Travel expenses are not reimbursable under this Contract.

13. USAC PROGRAM MANAGER AND CONTRACT MANAGER

The Program Manager ("PM") for the Contract is TBD, the USAC point of contact for overseeing the performance of the Services. USAC's Contracts Administrator ("CA") for the Contract is TBD, the USAC point of contact for contractual matters (e.g., contract modifications and other contractual matters).

14. USAC TECHNOLOGY AND EMAIL USE

For Contracts requiring access to USAC networks and systems, all Contractor Staff must use their USAC-issued technology to share and store all USAC documents for work purposes. Contractor Staff shall not use external technologies that are not approved by USAC to create, send or view USAC content, documents and/or material.

If USAC issues Contractor Staff an email address (@usac.org), Contractor Staff must use this email address to send and receive all USAC communications and material. USAC documents should not be forwarded or shared to non-USAC email addresses.

If confidential USAC information is sent to unauthorized individuals, Contractor must immediately inform their USAC point of contact and immediately complete and submit a Privacy Intake Form (provided upon request).

USAC documents shall not be stored in an unauthorized location, personal email, personal cloud, or any portable storage device.

USAC-issued property, including laptops, must not be left unattended and may not be used by anyone aside from the personnel assigned to the USAC-issued property. As part of the offboarding process, Contractor must return all USAC property—whether tangible or intangible—including all USAC Confidential Information and Materials in their possession. Contractor must provide written confirmation to USAC that it and its subcontractors have fully complied with this requirement within ten (10) calendar days. In the event of any damage, loss, or theft of tangible or intangible property, Contractor will be held responsible.

15. FOLLOWING PM@USAC POLICY

When applicable, Contractors serving in any capacity as part of a project team must employ PM@USAC as the required project management framework to the processes, procedures, tools, templates, and artifacts contained within PM@USAC. Any deviations or changes much be approved by PM@USAC.com.

PM@USAC, which is a slightly tailored version of Project Management Institute's PMBOK methodology, is the required project management framework to ensure all projects are conducted

in a disciplined, well-managed, and consistent manner that promotes the delivery of quality products and services to both internal and external stakeholders.

16. DOCUMENT LABELING AND MANAGEMENT

Contractors are responsible for the protection and proper disclosure of all information, data and documents in their possession or control. Every effort must be made to protect information, documents and all other property entrusted to Contractor. Every document must have the appropriate marking, such as Confidential/For Internal USAC Use Only.

Contractor must retain all USAC data and documents generated in accordance with USAC's record retention policy and provide those data and documents to USAC upon request or per stated submission instructions in USAC's policies. All retained USAC data and documents must be reasonably accessible and migratable from the system throughout the duration of the contract or required retention period. Upon contract expiration, USAC may request for Contractor to migrate any stored USAC data and documents to USAC in a format acceptable to USAC. Contractor shall not destroy documents without written approval from USAC.

Section C:
USAC Standard Terms and Conditions

1. DEFINITIONS

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

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

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

D. "Contract" means these USAC Terms and Conditions (including the attached USAC Standard Terms and Conditions Privacy and Security Addendum), and any documents attached to these USAC Terms and Conditions that constitutes the entire agreement between the parties with respect to the subject matter hereof.

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

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

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

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

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

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

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

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

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

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

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

P. "Privacy and Security Addendum" means the part of this document that includes most of the language regarding Contractor's obligations around protecting USAC Data.

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

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

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

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

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

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

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

X. "Sub-Recipient" means a partner, joint venturer, director, employee, agent, or subcontractor of a Recipient to whom a Recipient must disclose Confidential Information.

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

Z. "USAC" means Universal Service Administrative Company.

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

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

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

DD. "USF" means the Universal Service Fund.

2. TERM

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

3. ACCEPTANCE / REJECTION

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

A. Accept the Services and Deliverables; or

B. Reject the Services and Deliverables and advise Contractor of the reasons for the rejection.

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

USAC will reject any Service or Deliverable that does not conform to the acceptance criteria described in a statement of work or scope of work to the Contract. If rejected, Contractor must repair, correct, or replace nonconforming Deliverables or re-perform nonconforming Services, at no increase in Contract price. If repair, correction, replacement, or re-performance by Contractor does not cure the defects within thirty (30) calendar days or if curing the defects is not possible, USAC may terminate for cause under Section 12 of these USAC Standard Terms and Conditions, and in addition to any other remedies, may reduce the Contract price to deduct amounts for the defective work.

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

4. ENTIRE CONTRACT / BINDING EFFECT

The Contract supersedes and replaces all prior or contemporaneous representations, dealings, understandings, or agreements, written or oral, regarding such subject matter. In the event of any conflict between these USAC Standard Terms and Conditions and any other document made part of the Contract, the USAC Standard Terms and Conditions shall govern. The Contract shall be binding upon and shall inure to the benefit of the parties hereto and their respective successors and assignees.

5. MODIFICATIONS

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

6. INVOICES

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

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

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

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

7. FEES AND RATES INCLUSIVE OF ALL CHARGES AND TAXES

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

8. PAYMENT

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

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

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

9. ASSIGNMENT, DELEGATION, AND SUBCONTRACTING

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

10. REPORTS

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

11. TERMINATION FOR CONVENIENCE

USAC may terminate the Contract for any reason or no reason upon one (1) day prior written notice to Contractor without any liability or obligation thereafter. Subject to the terms of the Contract, Contractor shall be paid for all time actually spent performing the Services required by the Contract up to date of termination, plus reasonable charges that USAC, in its sole discretion, agrees in writing have resulted directly from the termination.

12. TERMINATION FOR CAUSE

Either party may terminate the Contract for cause upon providing the other party with a written notice. Such notice will provide the other party with a ten (10) day cure period. Upon the expiration of the ten (10) day cure period (during which the defaulting party does not provide a sufficient cure), the non-defaulting party may immediately thereafter terminate the Contract, in whole or in part, if the defaulting party continues to fail to comply with any term or condition of the Contract or fails to provide the non-defaulting party, upon request, with adequate assurances of future performance. In the event of termination for cause, the non-defaulting party shall be entitled to any and all rights and remedies provided by law or equity. If it is determined that USAC improperly terminated the Contract for cause, such termination shall be deemed a termination for convenience. In the event of partial termination, the defaulting party shall continue to perform the portion of the Services not terminated.

13. STOP WORK ORDER

USAC may, in its sole discretion and without further obligation or liability, issue a stop work order at any time during the Contract Term. Upon receipt of a stop work notice, or upon receipt of a notice of termination (for cause or convenience), unless otherwise directed by USAC in writing, Contractor shall, on the stop work date identified in the stop work or termination notice: (a) stop work, and cause Contractor Staff to stop work, to the extent specified in said notice; and (b) subject to the prior written approval of USAC, transfer title and/or applicable licenses, as appropriate, to USAC and deliver to USAC, or as directed by USAC, all USAC Data, Confidential Information, Software, Deliverable, or any Derivative Work to any of the preceding, whether completed or in process, for the work stopped. In the event of a stop work order, all deadlines in the Contract shall be extended on a day for day basis from such date, plus reasonable additional time, as agreed upon between the parties, acting in good faith, to allow Contractor to reconstitute its staff and resume the work.

14. LIMITATION OF LIABILITY

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

15. INDEMNITY

Contractor shall indemnify, hold harmless, and defend USAC and its directors, officers, employees, and agents against any and all demands, claims and liability, costs and expenses (including attorney's fees and court costs), directly or indirectly related to: (a) any claims or demands for actual or alleged direct or contributory infringement of, or inducement to infringe, or misappropriation of, any intellectual property, including, but not limited to, trade secret, patent, trademark, service mark, or copyright, arising out of or related to Contractor's performance of the Contract; (b) any claims or demands for personal injuries, death, or damage to tangible personal or real property to the extent caused by the intentional, reckless, or negligent acts or omissions of Contractor or Contractor Staff in connection with this Contract; and (c) any claims or demands of any nature whatsoever to the extent caused by Contractor's breach of any confidentiality, security, or privacy obligations set forth in these USAC Standard Terms and Conditions by Contractor or Contractor Staff; (d) Contractor's unauthorized use of USAC Software, USAC IT Systems, or USAC Data; (e) any breach of applicable law as described in Section 27 of these USAC Standard Terms and Conditions by Contractor or Contractor Staff; or (f) the negligent, reckless, illegal, or intentional acts or omissions of Contractor or Contractor Staff in connection with the performance of the Services.

16. CONFIDENTIAL INFORMATION

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

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

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

3. Information concerning USAC's relationships with other vendors or contractors, the FCC, USF Stakeholders, or financial institutions;
4. Information marked to indicate disclosure limitations such as "Confidential Information," "proprietary," "privileged," "not for public disclosure," "work product," etc.;

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

6. PII [defined in the USAC Standard Terms and Conditions Privacy and Security Addendum.]; and

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

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

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

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

E. *Exclusions*. If requested to disclose Confidential Information by an authorized governmental or judicial body, Recipient must promptly notify Discloser of the request, and to the extent that it may legally do so, Recipient must refrain from disclosure of the Confidential Information until Discloser has had sufficient time to take any action as it deems appropriate to protect the Confidential Information. In the event Confidential

Information of USAC is requested, Recipient must immediately notify USAC, with a copy to USAC's General Counsel, of the request. Neither Contractor nor Contractor Staff shall issue any public statement relating to or in any way disclosing any aspect of the Contract without the prior written consent of USAC. Notwithstanding anything herein to the contrary, USAC may, without notice to Contractor, provide the Contract, including Contractor's proposal information, and any information or USAC Data delivered, prepared, or developed by Contractor in the performance of the Contract to the FCC or other governmental or judicial body, and may publicly disclose basic information regarding the Contract, e.g., name of Contractor, price, basis for selection, description of Services/Deliverables and any provisions necessary for USAC to justify actions taken with respect to the Contract.

17. RETURN OR DESTRUCTION OF USAC DATA

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

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

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

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

E. *Destruction of Electronic Copies.* If Contractor destroys electronic copies in computer memory or any other type of media, destruction must be done pursuant to guidelines in NIST SP 800-88 Rev. 1 or the most current revision. ["NIST" is defined in the USAC Standard Terms and Conditions Privacy and Security Addendum.]

F. *No Other Use.* USAC Data is provided to Contractor solely for the purpose of rendering the Services, and USAC Data or any part thereof shall not be sold, assigned, leased, or otherwise transferred to any third party by Contractor (except as required to perform the Services or as otherwise authorized in the Contract), commingled with non-USAC Data, modified, decompiled, reverse engineered, or commercially exploited by or on behalf of Contractor, Contractor Staff, or any third party.

18. PROPRIETARY RIGHTS

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

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

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

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

19. RESPONSIBILITY FOR CONTRACTOR STAFF

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

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

20. KEY PERSONNEL

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

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

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

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

21. SHIPMENT/DELIVERY

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

22. INSURANCE

At its own expense, Contractor shall maintain sufficient insurance in amounts required by law or appropriate for the industry, whichever is greater, to protect and compensate USAC from all claims, risks, and damages/injuries that may arise under the Contract, including, as appropriate, worker's compensation, employer's liability, commercial general liability, commercial crime

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

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

23. CONFLICTS OF INTEREST

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

24. WAIVER

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

25. SEVERABILITY

The invalidity or unenforceability of any provisions of the Contract shall not affect the validity or enforceability of any other provision of the Contract, which shall remain in full force and effect. The parties further agree to negotiate replacement provisions for any unenforceable term that are as close as possible to the original term, and to change such original term only to the extent necessary to render the term valid and enforceable.

26. CHOICE OF LAW / CONSENT TO JURISDICTION

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

27. USAC AND APPLICABLE LAWS

USAC is not a federal agency, a government corporation, a government controlled corporation, or any other establishment in the Executive Branch of the United States government. USAC is not a contractor to the federal government and the Contract is not a subcontract under a federal prime contract. USAC conducts its procurements in accordance with the terms of a Memorandum of Understanding with the FCC, which requires USAC and its Contractors to adhere to the Procurement Regulations. Contractor shall comply with the Procurement Regulations and all applicable federal, state and local laws, executive orders, rules, regulations, declarations, decrees, directives, legislative enactments, orders, ordinances, common law, guidance, and other binding restriction or requirement of or by any governmental authority related to the Services or Contractor's performance of its obligations under this Contract, and includes without limitation FCC Orders; the rules, regulations and policies of the FCC; the Privacy Act of 1974; and the laws and guidelines named in the USAC Standard Terms and Conditions Privacy and Security Addendum.

28. RIGHTS IN THE EVENT OF BANKRUPTCY

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

parties further agree that, in the event of the commencement of bankruptcy proceedings by or against Contractor under the Code, USAC shall be entitled to retain all of its rights under the Contract and shall not, as a result of such proceedings, forfeit its rights to any USAC Data, Software, Deliverable, or any Derivative Work thereof.

29. NON EXCLUSIVITY

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

30. INDEPENDENT CONTRACTOR

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

31. TEMPORARY EXTENSION OF SERVICES

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

32. NOTICES

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

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

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

With a copy to:

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

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

33. SURVIVAL

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

34. FORCE MAJEURE

Neither party to this Contract is liable for any delays or failures in its performance hereunder resulting from circumstances or causes beyond its reasonable control, including, without limitation, force majeure acts of God (but excluding weather conditions regardless of severity), fires, accidents, epidemics, pandemics, riots, strikes, acts or threatened acts of terrorism, war or other violence, or any law, order or requirement of any governmental agency or authority (but excluding orders or requirements pertaining to tax liability). Upon the occurrence of a force majeure event, the non-performing party shall provide immediate notice to the other party and will be excused from any further performance of its obligations effected by the force majeure event for

so long as the event continues and such party continues to use commercially reasonable efforts to resume performance as soon as reasonably practicable, and continues to take reasonable steps to mitigate the impact on the other party. If such non-performance continues for more than ten (10) days, then the other party may terminate this Contract with at least one (1) day prior written notice to the other party. In the event that the force majeure event is a law, order, or requirement made by a government agency or authority related to USAC and the purposes of this Contract, USAC may immediately terminate this Contract without penalty upon written notification to Contractor.

35. EXECUTION / AUTHORITY

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

36. NATIONAL SECURITY SUPPLY CHAIN REQUIREMENTS

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

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

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

C. *Monitoring*. Contractor must actively monitor what entities have been finally designated by the FCC as a Covered Company and what equipment and services the FCC defines as Covered Equipment or Services and places on the Covered List. Contractor must actively monitor to ensure that no funds from USAC or other federal subsidies are used to purchase, obtain, maintain, or otherwise support any equipment or services produced or provided by a Covered Company from 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 36.D of these USAC Standard Terms and Conditions. Any such notification must have audit ready supporting evidence.

D. *Annual Inquiry & Certifications*. Contractor will conduct a Reasonable Inquiry upon execution of this Contract and no later than December 31 of each calendar year that the Contract is in effect. If Contractor, or any applicable subcontractor, is not in compliance with Section 36.B. of these USAC Standard Terms and Conditions, Contractor shall inform USAC and provide the following information in the certification:

(i) If for equipment produced or provided by a Covered Company or equipment on the Covered List:

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

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

a. If the service is related to item maintenance: A description of all such services provided (include on the item being maintained: brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable);
b. If the service is not associated with maintenance, the product service code of the service being provided; and

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

At USAC's discretion, and at any time during the performance of this contract, USAC may require Contractor to certify it, and all applicable subcontractors, are in compliance with Section 36.B of these USAC Standard Terms and Conditions. Contractor shall state in the certification that no funds from USAC have been used to purchase, obtain, maintain, or otherwise support any equipment or services produced by a Covered Company or Covered Equipment or Services on the Covered List.

Contractor shall retain supporting evidence for all certifications.

37. PROHIBITION ON A BYTEDANCE COVERED APPLICATION

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

1. *"Covered Application"* means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

2. *"Information Technology"* means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by USAC, if the equipment is used by USAC directly or is used by Contractor under this Contract with USAC that requires the use—

(a) Of that equipment; or

(b) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

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

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

B. *Prohibition*. Contractor is prohibited from having or using a Covered Application on any Information Technology owned or managed by USAC, or on any Information Technology used or provided by Contractor under this Contract, including equipment provided by Contractor Staff.

C. *Subcontracts.* Contractor shall insert the substance of this clause, including this subsection C, in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

38. ADDED SERVICES

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

39. PRIVACY AND SECURITY ADDENDUM

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

40. SECTION 508 STANDARDS

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

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

USAC STANDARD TERMS AND CONDITIONS

PRIVACY AND SECURITY ADDENDUM

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

1. DEFINITIONS

"Artificial Intelligence" or "AI"	A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.
"Authority to Operate" or "ATO"	The official management decision given by a USAC official or officials to authorize operation of an information system and to explicitly accept the risk to USAC operations (including mission, functions, image, or reputation), USAC assets, individuals, and other organizations based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.
"Contractor IT"	Any information technology device, software, hardware, equipment, system, and/or any IaaS, PaaS, or SaaS provided by a CSP that is owned or managed by Contractor, its agents, or subcontractors.
"Cloud Protocols"	A comprehensive information security program governing standard technical configurations, platforms, or sets of procedures used in connection with the Services operated in cloud infrastructure environments.
"Cloud Service Offering"	A service from a cloud service provider. FedRAMP categorizes Cloud Service Offerings as one of the following: IaaS, PaaS, or SaaS.
"Cloud Service Provider" or "CSP"	A provider of IT infrastructure, product, or SaaS to be acquired by a user of IT services.
"COTS"	Commercial off-the-shelf Software, which is Software, hardware, and information technology products that (1) already exist, (2) are available from commercial sources, (3) are ready-made, and (4) are available for purchase by the general public.

"Cybersecurity/Data Breach"	A successful incident in which sensitive, confidential, or otherwise protected system/data has been accessed and/or disclosed in an unauthorized fashion. For example, a brute force attack against a protected system, attempting to guess multiple usernames and passwords, is a Cybersecurity Incident, but cannot be defined as a Cybersecurity/Data Breach unless the attacker succeeded in guessing a password. If a Cybersecurity Incident grants the attacker access to protected systems, it may qualify as a Cybersecurity/Data Breach. If the attacker obtained access to USAC Data, it is a Cybersecurity/Data Breach. Not every Cybersecurity Incident is a Cybersecurity/Data Breach, Privacy Incident, or a Privacy Breach. Most Cybersecurity Incidents do not result in an actual Cybersecurity/Data Breach. Examples of Cybersecurity/Data Breaches may include, but are not limited to: • Bringing down the USAC.org website (for example, through a Denial of Service (DoS) Attack. • Employee causes ransomware to be installed and encrypts computer or entire network (Phishing Attack, DoS Attack) • Attacker obtains USAC Data through unauthorized access. • Unencrypted USAC Data being disseminated through peer-to-peer file sharing service.
"Cybersecurity Incident"	An event that attempts to or successfully compromises the integrity, confidentiality, and/or availability of an information asset or USAC Data. A Cybersecurity Incident could be either intentional or accidental in nature. Cybersecurity incidents hereafter may be referred to as a "Cyber Incident" or "Incident".

"Data at Rest"	State of data while it is on the device that stores it, or data that has reached a destination and is not being accessed or used. This term is primarily used in the context of data encryption. It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory waiting to be read or updated. It does not include data in use while it is being processed, accessed, or read where it must be decrypted to be used.
"Data in Transit"	Data transmitted via email, web, collaborative work applications, instant messaging, or any type of private or public communication channel. This term is primarily used in the context of data encryption. It includes all data moving between systems or devices on networks. It does not include data in use while it is being processed, accessed, or read where it must be decrypted to be used.
"Data Leakage"	The inadvertent exposure of data beyond its controlled environment or intended usage, such as a lost or stolen laptop, an employee storing files using an Internet storage application, or an employee saving files on a USB drive to take home.
"Data Loss"	The exposure of proprietary, sensitive, or classified information through either Data Theft or Data Leakage. This includes the intentional or unintentional destruction of information, caused by people and or processes from within or outside of an organization. In a Cybersecurity/Data Breach or Privacy Breach the data is compromised, but Data Loss further describes damage to the integrity, completeness, or control of the data.
"Data Safeguards"	Protections that safeguard USAC Data against destruction, loss, damage, corruption, alteration, loss of integrity, commingling, or unauthorized access or Processing.
"Data Security Laws"	FISMA, 44 U.S.C. § 3541, et seq., the Privacy Act as amended (as may be applicable), and NIST SP 800-53 Rev 5. PII protections in accordance with all federal and USAC requirements, including, but not limited to, OMB Memoranda M-17-12 and guidance from NIST including, but not limited to, NIST SP 800-53 Rev 5 and NIST SP 800-61 Rev 2 (or most current version), and FIPS 140-3. Any federally mandated information security and privacy requirements not described herein.
"Data Theft"	The deliberate or intentional act of stealing information such that controlled data is intentionally stolen or exposed, such as in cases of espionage or employee disgruntlement.

"Event"	An exception to the normal operation of IT infrastructure, systems, services, or privacy. Not all Events become a Cybersecurity Incident or Privacy Incident. Cybersecurity Incidents and Privacy Incidents are Events which can represent a threat, an attack, or a breach.
"Exfiltration"	The unauthorized transfer of information from USAC IT Systems.
"FedRAMP-Authorized," or "FedRAMP Authorization"	A term used to designate a Cloud Service Offering from a CSP that satisfies the security assessment, authorization, and continuous monitoring requirements of the Federal Risk and Authorization Management Program ("FedRAMP"), a US government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies; see FedRAMP.gov.
"FIPS"	Federal Information Processing Standards. FIPS are standards and guidelines for computer systems that are developed by NIST in accordance with FISMA and approved by the Secretary of Commerce. These standards and guidelines are developed when there are no acceptable industry standards or solutions for a particular requirement.
"FISMA"	The Federal Information Security Management Act, 44 U.S.C. §3541, *et seq*., as amended by the Federal Information Security Modernization Act of 2014, and their implementing and successor regulations.
"IaaS"	Infrastructure as a service.

"Malicious Code" or "Malware"	Any software, hardware, 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) designed to (i) disrupt, disable, deactivate, interfere with, or otherwise compromise USAC IT Systems, or (ii) access, modify, disclose, transmit, or delete PII, Confidential Information, or USAC Data; or (b) either inadvertently or upon the occurrence of a certain event, compromises the confidentiality, integrity, privacy, security, or availability of PII, Confidential Information, USAC Data, or USAC IT Systems. Examples of Malicious Code include, but are not limited to, viruses, worms, bugs, ransomware, spyware, bots, backdoors, devices, root kits, and Trojan Horses. For purposes of this definition, "root kits" are a set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means.
"Malicious Cyber Activity"	Any activity, other than those activities authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information systems, communications systems, networks, or physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.
"Multifactor Authentication"	A type of authentication using two or more factors to achieve verification of the identity of a user, process, or device as a prerequisite to allowing access to an information system. A user is granted access only after successfully presenting two or more pieces of evidence to an authentication mechanism. Factors include, but are not limited to: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); and/or (iii) something you are (e.g., biometric).
"NIST" and "NIST SP"	NIST means the National Institute of Standards and Technology, part of the U.S. Department of Commerce. NIST SP means a special publication published by NIST.
"OMB"	Office of Management and Budget.
"PaaS"	Platform as a service.

"Personally Identifiable Information" or "PII"	Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII include name, address, telephone number, date and place of birth, mother's maiden name, biometric records, social security number, etc.
"PIN"	Personal Identification Number
"Privacy Breach"	A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to PII. When PII is involved in a Cybersecurity/Data Breach it then becomes a Privacy Breach.
"Privacy Incident"	An unauthorized use or disclosure of confidential, sensitive, or regulated data, like USAC Data, PII, or confidential commercial information. For example, an unauthorized user gains access to a system containing PII and exfiltrates the PII.
"Process" or "Processing"	Any operation or set of operations that is performed using USAC Data, whether or not by automatic means, including, but not limited to, collection, retention, logging, generation, transformation, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, making available, alignment, combination, blocking, deleting, erasure, destruction, transfer, or disposal.
"Risk Management Framework" or "RMF"	A seven (7) step process that any organization can use to manage information security and privacy risk for organizations and systems and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of FISMA.
"SaaS"	Software as a service.

2. SECURITY PROVISIONS

2.1 Data Security Laws Compliance. Contractor shall comply with the Data Security Laws. For any Contractor IT using a Cloud Service Offering that accesses, stores, or otherwise processes USAC Data, and/or PII, Contractor shall provide documentation and proof of FedRAMP Authorization for use at a moderate risk before any such cloud-based Service may be used. USAC reserves the right to inspect the Authority to Operate or the complete package of documents for any Cloud Service Offering with agency accreditation.

2.2 Contractor Compliance Generally. Throughout the Contract Term, Contractor shall comply with: (i) USAC's information privacy and IT security policies; and (ii) the

prevailing standards of care and best practices regarding information privacy and IT security to the extent they meet or exceed the requirements of the Data Security Laws, the aforementioned USAC policies, or the obligations set forth in this Privacy and Security Addendum or the USAC Standard Terms and Conditions.

2.3 Contractor Duties Prior to Delivering Services. Prior to delivering the Services or enabling data-sharing or interoperability of any kind with USAC IT Systems, Contractor shall: (i) demonstrate Contractor system is compliant with FISMA and NIST SP 800-53 Rev. 5 and has received an Authority to Operate by Contractor's authorizing official after following the steps laid out in the NIST risk management framework by providing evidence thereof; (ii) work with USAC to document, establish and enable the effective and secure integration of any gateways or data transmission mechanisms necessary for the parties to perform their obligations under the Data Security Laws; (iii) complete any security questionnaires, IT rules of behavior, certifications, assessments, or workforce training reasonably requested by USAC in a timely manner; and (iv) receive prior written authorization from USAC to access USAC IT Systems from USAC. If at any time USAC determines that the establishment of such gateways or data transmission mechanisms is reasonably required to securely access the Services, their establishment shall be at Contractor's sole cost and expense. Under no circumstances shall USAC's written authorization to access USAC IT Systems serve as a representation or warranty by USAC that such access is secure or as a waiver of any rights in this Privacy and Security Addendum or the USAC Standard Terms and Conditions. Failure to satisfy the conditions set forth in subsections (i) – (iv) herein to USAC's reasonable satisfaction shall be considered a material breach of the USAC Standard Terms and Conditions by Contractor.

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

2.5 Compliance Plan. In providing the Services, Contractor's Data Safeguards shall be no less rigorous than the most protective of: (a) the requirements of applicable Law; (b) the specific standards set forth in this Article; and (c) the applicable USAC standards relating to data security. The parties shall execute an interconnection security agreement prior to

any required establishment of direct interconnection between Contractor IT and USAC IT Systems.

2.6 PII. Contractor shall ensure that: (i) PII shall be protected in accordance with all laws and USAC requirements, including, without limitation, relevant: (a) OMB Memorandum M-17-12; (b) guidance from the NIST including without limitation the most current revision of NIST SP 800-53 Rev. 5; and (c) FCC requirements or the most current replacement of the above; (ii) to the extent that cloud-based Services are to be employed by Contractor and interact with USAC Data, Contractor shall provide documentation and proof of FedRAMP-Authorization to demonstrate compliance, and such Services shall be certified by FedRAMP for use at a moderate risk by the time the cloud-based Services are implemented (USAC reserves the right to inspect the Authority to Operate or the complete package of documents for those with agency accreditation); and (iii) all Cybersecurity Incidents or Privacy Incidents resulting in any interruption to system services, including the disclosure of PII, shall be tracked in accordance with NIST SP 800-53 Rev. 5, NIST SP 800-61, and OMB Memorandum M-17-12.

2.7 Contractor Responsible for Contract Staff. Contractor shall ensure that all Contract Staff will be bound by the same or substantially similar restrictions on collection, use, disclosure, and retention of PII, Confidential Information, USAC Data, and USAC Software. Contractor shall be responsible for any breach of data security or privacy-related obligations by any Contract Staff and shall fully indemnify USAC for any damages incurred as a result of such breach. Contractor will be required to provide annual information security and privacy awareness training to all Contract Staff that will be working under the USAC Standard Terms and Conditions prior to having access to USAC Data or to USAC IT Systems. All Contract Staff will also be required to sign USAC's IT rules of behavior as well as confidentiality and non-disclosure agreements as required by third parties and USAC.

2.8 Vendor Insider Threat Program. Vendor will submit Vendor's insider threat program (as required by NIST 800-53 Rev. 5 (see controls PM-12, IR-4(6), IR-4(7), and SI-4(12)) to USAC's Chief Privacy Officer and USAC's Chief Information Security Officer within ninety (90) days of the Effective Date of the Contract. If USAC has any questions regarding Vendor's insider threat program, Vendor will make Contract Staff knowledgeable of Vendor's insider threat program available to USAC upon USAC's request.

2.9 Encryption and Secure Storage. PII must be encrypted at all times in accordance with FIPS 140-3 standards. This encryption requirement includes both Data at Rest and Data in Transit. Any PII that is retained in documents or other physical formats must be stored in a secured location and with limited access. The standard for disposal of PII requires practices that are adequate to protect against unauthorized access or use of the PII, including at minimum adhering to the provisions of the USAC Terms and Conditions and this Privacy and Security Addendum.

2.10 Further Requirements. Contractor's applications, processes, and systems used in providing the Services shall be approved by USAC's IT security team and shall comply with FISMA, NIST, and OMB requirements. Contractor shall demonstrate Authority to Operate for any system that will temporarily or permanently house USAC Data, in compliance with NIST standards, and will provide all relevant documentation as defined in the NIST RMF lifecycle therein. Contractor further agrees to provide any assistance requested by USAC to enable Contractor or USAC to comply with FISMA requirements, including, without limitation, at Contractor's expense, providing USAC with periodic documentation and reports demonstrating FISMA compliance, system accreditation, and correction of any weakness or deficiency (as defined by FISMA) attributable to Contractor that would prevent Contractor or USAC from complying with FISMA. Contractor shall be responsible at its sole expense to remediate any FISMA noncompliance of its systems or the Services. No less than annually, Contractor shall write, review, and update an assessment of its compliance with all applicable federal mandates and other industry-accepted standards as set forth in this Article to ensure adherence thereto. Contractor will also perform any and all activities needed to ensure continued compliance with all federal mandates and other industry-accepted standards as set forth in this Article. *[This provision is applicable to contracts for procuring new information technology systems/tools only]*

2.11 Contractor Assumption of the Risk. Contractor agrees that access to PII, USAC Data, Confidential Information, and USAC IT Systems is at USAC's sole discretion, and that Contractor's access to such systems or information may be conditioned, revoked or denied by USAC at any time, for any reason, without any liability whatsoever to USAC. Access to USAC IT Systems by Contractor and Contract Staff, including any data-sharing or interoperability between USAC and Contractor, shall be for the sole purpose of providing the Services. Contractor agrees that: (i) USAC IT Systems are owned solely by USAC; (ii) USAC will monitor the use of USAC IT Systems; (iii) neither Contractor nor Contract Staff have any expectation of privacy with regard to USAC IT Systems; and (iv) all information appearing on USAC IT Systems (except for information publicly disclosed by USAC) will be considered Confidential Information. Contractor will not use USAC IT Systems except as expressly authorized by USAC. USAC requires that Contract Staff use a USAC.org email address when providing Services. Contractor agrees that its use of, and access to, USAC IT Systems is completely at its own risk.

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

2.13 Performance Within United States. All Services must be performed within the United States. This requirement is inclusive of: (a) work related to the Services performed by all Contract Staff; and (b) storage and/or processing of data and/or other virtual Services (such as cloud storage, remote data processing, *etc*.).

2.14 Cybersecurity Incidents and Privacy Incidents

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

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

2.14.3 Contractor Responsibilities Prior-to and After Cybersecurity Incident or Privacy Incident. Contractor, working with USAC, shall use its best efforts to mitigate and eliminate the effects of the Cybersecurity Incident or Privacy Incident on USAC and, if the Cybersecurity Incident or Privacy Incident causes any loss of operational efficiency, loss of data, or unauthorized disclosure, Contractor will assist USAC in mitigating or restoring such losses or disclosures. Contractor agrees to fully cooperate with USAC in the investigation of the Cybersecurity Incident or Privacy Incident (including participating in any needed forensic investigation and law enforcement investigations) and to participate in, to the extent directed by USAC, the notification of individuals, the media, the FCC, or third parties. Contractor shall promptly respond to USAC's questions regarding the Cybersecurity Incident or Privacy Incident and coordinate with Contract Staff if required to mitigate the harm. To the extent USAC determines necessary, USAC agrees to provide reasonable access to the affected systems in order for Contractor to assist in such restoration of efficiency or data. Notwithstanding anything to the contrary in the USAC Standard Terms and Conditions, if the Cybersecurity Incident or Privacy Incident

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

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

2.16 Security Audit. USAC or its designated USAC auditor may, at USAC's expense and at any time, perform an audit of the security policies and procedures implemented by Contractor and in effect at Contractor locations. Contractor is responsible for remediation of any identified weakness or findings of noncompliance.

2.17 Security and Privacy Assessments. Contractor shall provide support for assessments of FISMA compliance on an annual basis. Security and privacy assessments may include, but are not limited to, third party assessments to achieve FISMA ATO or to maintain continuous monitoring and ongoing authorization of a Contractor IT system in compliance with the RMF and controls described in NIST SP 800-53 Rev 5. The assessment process may also include security penetration testing to identify additional vulnerabilities through ethical hacking and compliance challenging techniques. Assessments shall include but shall not be limited to: (a) Contractor's documented and demonstrated internal controls and procedures related to the Services; (b) cooperation with USAC IT security or privacy staff in connection with testing the effectiveness of such controls and procedures; (c) making at least quarterly representations to USAC regarding any significant changes to such controls and procedures; (d) documenting and tracking all identified material weaknesses or deficiencies reported by an assessment, penetration test, Cybersecurity Incident, Privacy Incident, or any other deficiency that would prevent USAC from complying with law, using a Plan of Action and Milestones ("POA&M") process; and (e) cooperating with USAC auditors in connection with the issuance of the reports described in Section 2.20 of this Privacy and Security Addendum. Contractor shall promptly remediate any weakness identified in any assessment, in no event later than recommended or demanded by the assessors. *[This provision is applicable to contracts for procuring new information technology systems/tools only]*

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

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

2.20 Additional Requirements for Services in Contractor IT

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

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

- Contractor shall maintain Contractor IT used by Contractor in performance of the Services. USAC may require Contractor to respond to the information security questionnaires regarding Contractor's information security policies and practices. USAC will conduct its information security review, if required, with reference to the responses Contractor provides to such information security questionnaires. At USAC's request, Contractor shall also respond promptly (within 10 business days) to any new or supplemental information security questions that USAC may require of Contractor during performance. USAC may terminate the Contract upon notice if Contractor fails to provide a timely response to requests for new or supplemental information security information or if USAC determines that Contractor's information security policies or practices increase risk to USAC in a manner unacceptable to USAC.

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

- Contractor shall maintain administrative, technical, physical, and procedural information security controls as demonstrated in Service Organization Controls ("SOC") 2 Type II reports. Contractor shall maintain these controls and notify USAC of any changes to its compliance. Contractor shall provide USAC with its most current SOC 2 Type II report within ten (10) calendar days of the Effective Date

- On an annual basis, upon written request, Contractor will provide USAC with the most current versions of following:

  - Contractor security policies referenced in Section 2.4 of this Privacy and Security Addendum;
  - Standard Information Gathering (SIG) Lite documentation;
  - SOC 2 Type II report;
  - System ATO(s) or evidence of effective Information Security Continuous Monitoring (ISCM) in compliance with FISMA and NIST SP 800-53 Rev. 5;
  - ISO 27001 certifications.

[This provision is applicable to contracts for procuring new information technology systems/tools only]

3. TECHNOLOGY CONSIDERATIONS

3.1 Deployment in Cloud. Contractor shall ensure that SaaS, PaaS, or IaaS Cloud Service Offerings, or COTS, deployed in Contractor IT cloud or on any USAC-acquired CSP infrastructure, satisfies the following requirements:

3.1.1 The Software must be able to utilize USAC's instance of OKTA's identity and access management software for user authentication and provisioning. OKTA is a FedRAMP Authorized CSP identity and access management product used by USAC.

3.1.2 Any USAC Data stored in a database that is a component of a CSP SaaS, PaaS, or IaaS, or a COTS, must be readily available to USAC in industry standard formats that enable USAC to access, copy, or transfer USAC Data as required.

3.1.3 Any SaaS, PaaS, or IaaS Software must maintain the Authority to Operate and FedRAMP Authorization for the Contract Term.

3.2 Custom Software. Contractor shall ensure that any custom Software developed and/or deployed for USAC, whether on USAC premise, on a USAC or Contractor cloud, or on a hybrid infrastructure:

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

3.2.2 Reuses available USAC technology services (including microservices and application programming interfaces) unless Contractor demonstrates in writing that those services are unable to meet the requirements and USAC agrees to the substitute solution in writing with Contractor.

3.2.3 Uses the USAC technical stack unless Contractor demonstrates in writing that those components are unable to meet the requirements and USAC agrees in writing with Contractor. Details of USAC's technical stack and service architecture will be provided as appropriate.

3.3 Artificial Intelligence. Contractor shall not use, implement, build, or deploy AI tools, services, or code of any type without prior written approval from USAC. Any proposed AI use in solutions, processing, document reviews/analysis, or management of USAC systems or processes must be both submitted in writing and receive written approval prior to use. In addition:

3.3.1 USAC Data Restrictions. Use, uploading, input, or processing of USAC Data, Confidential Information, and/or PII in any AI tool (including third-party or public models) requires prior written authorization from USAC and must comply with all applicable privacy laws and USAC security requirements as specified in this Privacy and Security Addendum.

3.3.2 Required Disclosures. For any AI approved under this provision, Contractor must disclose in writing: the use, limitations, and risks related to USAC data or connections for any approved AI capability deployed in products, services, or development, to include training data sources, learning cutoff dates, and model limitations. Contractor must promptly notify USAC in writing of any material changes to any items listed in this subsection 3.3.2.

3.3.3 Human Oversight. Any AI may support, but never replace or override, USAC staff responsible for decision-making, especially for areas that affect program beneficiaries or operations.

3.3.4 Prohibited Autonomous AI. Contractor shall not develop or deploy AI for autonomous decisions without human review and oversight in sensitive areas, including public benefits, human resources, hiring practices, legal determinations, case outcomes, or surveillance.

3.3.5 Output Review and Controls. All approved AI deployments must include processes for: (i) human review of outputs; (ii) verifying accuracy, compliance, and lack of bias; and (iii) logging AI activity for audits, consistent with USAC's retention policies.

3.3.6 Subcontractor and Third-Party Compliance. Contractor must ensure AI tools used by its subcontractors and third parties comply with this Section 3.3. Contractor remains responsible for their AI-related activities.

3.3.7 Incident Reporting. Contractor must promptly notify USAC (within one (1) hour) of any unauthorized AI use, AI security incident, data misuse, or harmful/malfunctioning AI output affecting USAC interests. Contractor must comply with investigation/mediation.

3.3.8 Policy Compliance. Contractor shall comply with USAC's Secure and Trustworthy Artificial Intelligence Policy, plus all related USAC privacy/security policies, including this Privacy and Security Addendum, and applicable laws. This Section 3.3 controls over conflicting Contractor policies.

4. MALICIOUS CODE AND MALICIOUS CYBER ACTIVITIES

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

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

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

SECTION D: Attachments

Attachment List:

- Attachment 1: Bid Sheet
- Attachment 2: Confidentiality Agreement

SECTION E:
Instructions and Evaluation Criteria

1. GENERAL

A. CONTRACT TERMS AND CONDITIONS

The Contract(s) awarded as a result of this RFP will be governed by, and subject to, the requirements of all Sections of this RFP, including any attachments listed in Section D. Offeror's submission of a proposal constitutes Offeror's agreement to the RFP and its precedence over any other terms, requirements, or conditions proposed by Offeror. Offeror's submission must include a statement certifying that the USAC Standard Terms and Conditions set forth in this RFP have been reviewed by Offeror's office of general counsel (or equivalent legal representative).

Offeror's proposal may identify deviations from, or revisions, exceptions or additional terms (collectively "exceptions") to the RFP, but only if such exceptions are clearly identified in a separate Attachment to the proposal, "Exceptions to RFP Terms." Proposals that include material exceptions to the RFP may be considered unacceptable and render Offeror ineligible for award unless the Offeror withdraws or modifies any unacceptable exceptions prior to USAC's selection of the successful Offeror for award. USAC will only review and may consider changes or additions to the RFP that are included in Offeror's proposal. USAC reserves the right to eliminate a proposal from the evaluation process that includes material or unacceptable exceptions with or without notice to the offeror. After selection of the awardee, USAC will not consider or negotiate any exceptions to the RFP.

B. PERIOD FOR ACCEPTANCE OF OFFERS

Offeror agrees to hold the pricing in its offer firm for one hundred twenty (120) calendar days from the date specified for receipt of offers unless another time period is specified in an addendum to the solicitation.

Proposals must:

- Concisely address USAC's requirements, as set forth in Section B: Statement of Work, and should not contain a significant amount of corporate boilerplate marketing information.
- Be submitted to USAC Procurement Department, no later than **11:00 AM ET on June 10, 2026** ("Proposal Due Date").
- Be submitted in the form of one electronic copy submitted to Procurement@usac.org with the designated procurement agent in copy. The subject line for all email communication related to this solicitation should **only** state the Solicitation Number, IT-26-073, 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 27, 2026	RFP Released
May 6, 2026	Virtual Offeror's Conference
May 11, 2026	Questions due to USAC by 11:00 AM ET at Procurement@usac.org
May 21~~15~~, 2026	Q&A Released to Potential Offerors
June 10, 2026	Proposal Due to USAC by 11:00 AM ET at Procurement@usac.org
August 2026	Anticipated Award Date

Due to the importance of this procurement and USAC's desire to ensure that potential Offerors have all the relevant information available to respond to this solicitation, USAC will host a 1-hour Offeror's Conference on May 6, 2026 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 Offeror's Conference, Offerors must complete Attachment 2: Confidentiality Agreement and submit to Procurement@usac.org with a copy to Anthony.Smith@usac.org along with the names and email addresses of requested attendees. USAC will promptly review each request and will notify the potential bidder with the conference information. Offerors may also submit a list of questions to be addressed by USAC during the Offeror's Conference.

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 Procurement@usac.org with a copy to Anthony.Smith@usac.org no later than **May 11, 2026 by 11:00 AM ET**. USAC plans to post all questions and responses under this procurement on our website by **May 21~~15~~, 12~~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 either make a single-award or multiple-awards. USAC intends to award a Contract to the responsible Offeror(s) whose proposal represents the best overall value. USAC may reject any or all offers if such action is in the public's or USAC's interest; accept other than the lowest offers; and waive informalities and minor irregularities in offers received.

3. IDENTIFICATION OF CONFIDENTIAL INFORMATION

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

4. PROPOSAL FORMAT

Proposals shall be presented in four separate volumes:

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

5. PROPOSAL COVER PAGE

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

- The name of Offeror's organization,
- Offeror's contact name,
- Offeror's contact information (address, telephone number, email address, website address),
- Offeror's Unique Entity ID number,
- The date of submittal,
- A statement verifying the proposal is valid for a period of one hundred twenty (120) days, and
- The signature of a duly authorized Offeror representative.

6. PROPOSAL CONTENT

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

A. Corporate Information (Volume 1)

1. A cover page, as outlined above.

2. *Executive Summary*. This section shall summarize all key features of the proposal, affiliated individuals, or firms that Offeror proposes to assist in this engagement. Pricing information shall not appear in the Executive Summary.

3. *Confidentiality and Information Security*. Offeror must explain in detail how they will establish and maintain safeguards to protect the confidentiality and integrity of USAC Confidential Information in their possession as required by the solicitation.

4. *Conflict of Interest*. Offeror must provide a statement regarding any known conflicts of interest. USAC is the appointed neutral administrator of the federal USF. USAC is governed by a Board of Directors comprised of various stakeholders in the universal service programs and is prohibited from advocating positions on universal service policy matters. Because of USAC's unique role as neutral administrator, it is essential that any contractor providing assistance to USAC in administering the USF maintain the same neutrality, both in fact and in appearance.

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

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

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

B. Technical Capability (Volume 2)

This volume must include:

1. A cover page, as outlined above.

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

   Use of Artificial Intelligence: USAC will evaluate Offeror's proposed use of Artificial Intelligence ("AI") that complies with Section 3.3 of the Privacy and Security Addendum of USAC's Standard Terms and Conditions. Offeror must provide an in-depth overview of the proposed use of AI in Offeror's technical approach. Offeror must describe how and in what circumstances AI will be used to perform the Services specified in Section B of this RFP. Offeror's proposal submission should include separate versions of **Attachment 1: Bid Sheet** for scenarios with and without the use of AI. Offeror will not be permitted to use, implement, build, or deploy AI tools, services, or code of any type without prior written approval from USAC.

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

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

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

4. **Key Personnel:** Identify by name all Key Personnel. Describe the technical knowledge of and experience of proposed personnel in the requested Services with respect to, but not limited to, experience and qualifications including depth of knowledge, expertise and number of years. Indicate any other personnel that will be assigned to USAC and his/her role on the contract. Provide a brief summary of each of these professional staff members' qualifications to include education and all relevant experience.

a. Submit resumes for all Key Personnel, as an attachment (**Attachment A**) to the technical volume, no longer than two (2) pages in length per resume.

b. If Offeror, at time of proposal and prior to the award of the contract, has information that any such Key Personnel anticipate terminating his or her employment or affiliation with Offeror, Offeror shall identify such personnel and include the expected termination date in the proposal.

C. Past Performance Information (Volume 3)

This volume must include:

1. A cover page, as outlined above.

2. Description of Offeror's recent experience providing the related services as detailed in Section B of this RFP. Provide examples of the projects and personnel to include types of positions and length of assignments.

3. A list of 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 for each project discussed. A past performance description will consist of: (i) an overview of the engagement, (ii) a description of the scope of work performed, (iii) its relevance to this effort, and (iv) the results achieved. This is the time to identify any unique characteristics of the project, problems encountered, and corrective actions taken. Each overview shall not exceed one (1) page.

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

D. Price Proposal (Volume 4)

This volume must include:

1. A cover page, as outlined above.

2. Completed pricing information in **Attachment 1: Bid Sheet**.
   a. The proposed price must be *fully loaded* and must include wages, overhead, general, and administrative expenses, taxes, and profit.

E. Presentation and Page Limitations

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

2. Page Limitation

   Page count for each volume, exincluding the cover page, may not exceed the below:
   a. Volume 1 – Corporate Information; may not exceed four (4) pages.
   b. Volume 2 – Technical; may not exceed sixteen twelve (126) pages; however, excluding **Attachment A** (Resumes).
   c. Volume 3 – Past performance information; may not exceed five (5) pages.
   d. Volume 4 – Price; may not exceed four (4) pages.

Any proposals received exceeding the page count will be considered technically unacceptable and may not receive further consideration. Additional pages, such as table of contents, disclosure page, etc., shall be included in the page limit for each volume.

7. EVALUATION

USAC intends to either make a single-award or multiple-awards resulting from this solicitation to the responsible Offeror(s) whose offer conforming to the solicitation will be most advantageous to USAC, price and other factors considered. Offerors will be evaluated based on their capability to contribute expertise and services in support of USAC's IT continuity of security and privacy compliance, USAC's IT architectural improvements to meet Zero Trust guidance, and improvements in USAC's IT maturity leveraging technological innovation as a strategic factor for this procurement. Offerors showcasing deep experience delivering innovation for relevant prior engagements to improve IT environments for security and privacy compliance, security operations, and Zero Trust Architecture implementation will receive higher evaluation consideration.

The following factors shall be used to evaluate offers and select the awardee: Technical, Past Performance, and Price.

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

2. **Experience and Past Performance:** Experience and past performance information will be evaluated to assess the risks associated with Offeror's performance of this effort, considering the relevance, how recent the project is (no older than three (3) years from the date of the solicitation), and quality of Offeror's past performance on past or current contracts for the same or similar services. Offeror's past performance will be evaluated based on Offeror's discussion of its past performance for similar efforts, information obtained from past performance references (including detailed references for Offeror's proposed teaming partner(s) and/or subcontractor(s), as applicable), and information that may be obtained from any other sources (including government databases and contracts listed in Offeror's proposal that are not identified as references).

3. **Price Evaluation:** USAC will evaluate price based on the firm fixed price listed in **Attachment 1: Bid Sheet**. In addition to considering the total prices of Offerors when making the award, USAC will also evaluate whether the proposed prices are realistic (i.e., reasonably sufficient to perform the requirements) and reasonable. Proposals containing prices that are determined to be unrealistic or unreasonable will not be considered for award.

8. DOWN-SELECT PROCESS

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

9. RESPONSIBILITY DETERMINATION

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

1. Offeror has sufficient resources to perform the Services described in the RFP;
2. Offeror has a satisfactory record of performance, integrity, and business ethics;
3. Offeror has the accounting systems and internal controls, quality assurance processes, and organizational structure and experience necessary to assure that contract work will be properly performed and accurately invoiced;
4. Offeror has the facilities, and technical and personnel resources required to perform the contract;
5. Offeror is not excluded from government contracting, as listed on the excluded parties list in https://www.sam.gov; and
6. Offeror has an active registration in https://www.sam.gov.

Attachment 1

Bid Sheet (Attached Separately)