Universal Service Administrative Co. (USAC)
IT-23-053 – Chief Information Security Officer (CISO) Advisory Services
Questions & Answers

Q#	Question	Answer
1	Is there an incumbent on this contract? If so, please provide the incumbent name, current contract number, Period of performance, value of the contract.	USAC does not provide information regarding incumbent contractors.
2	If new then please provide the estimated level of effort?	Vendors should determine the estimated level of effort and submit a proposal based on the requirements stated in the RFP.
3	General question (all volumes) - Is the cover page, which is required for each Volume of the proposal, inclusive of the page counts dictated within the page limitations described on pages 62 and 63 of the RFP?	As specified in the RFP on Page 62, the page limit for each volume includes the cover page.
4	Pricing Question - Is the Bid Sheet (attachment 1) included in the page limitations described on pages 62 and 63 of the RFP?	The Bid Sheet does not count toward the page limits if submitted as a separate Excel attachment as an addition to Volume 4.
5	Can USAC elaborate whether all the scope defined in the PWS is currently being performed by a single vendor or multiple vendors? Can USAC provide the relevant contract details for each incumbent?	Please see response to Question #1.
6	Is there an incumbent or incumbents performing similar advisory work for USAC, and if so who is performing the work related to the SOW and what is the current value of the contract(s)?	Please see response to Question #1.
7	Of the approximate 25-30+ information systems referenced in the SOW Overview (p. 6), is the contractor to perform ISSO or ISSE duties in support of Assessment and Authorization (A&A) for each (e.g., IA documentation, security controls selection and implementation, security requirements, POA&M management, Continuous Monitoring, and other RMF activities)?	No, that is not in scope of this solicitation.

Q#	Question	Answer
8	Per SOW 6.E (contractor visitor status, p. 8), how many dedicated seats are available for the awardee's staff at USAC HQ in support of the contract? Because contractors are treated as visitors, are these "hot seats" or can contractor staff be assigned to occupy them for the days they are on location?	Please see response to Question #2. Additionally, on-site workspace will be allocated for all Contractor Staff, as needed. Contractor Staff will be able to reserve workspace 1-2 weeks prior to their scheduled workdays at USAC HQ.
9	Does USAC currently have a formalized or draft Cybersecurity Program, including draft plans and in-place leadership for the major elements of the program?	All existing artifacts will be provided to the Contractor after award and contract kick-off.
10	Do either of the roadmaps (strategic or tactical, SOW 7.A.c, p. 11) also include the need to meet EO 14028 with near and long term roadmaps to implementing Zero Trust within USAC and/or related FCC IT systems, networks, or assets?	The development of detailed roadmap(s) related to Zero Trust Architecture will be provided by separate team(s). However, the expectation is that the strategic and tactical roadmaps will be inclusive of all Information Security Program activities, including adherence to all relevant Federal guidance and directives.
11	Is the contractor expected to perform Incident Response/Incident Handling activities at the tactical level (e.g., protect, detect, triage, analyze, contain, mitigate, report, etc.) or does the contractor solely develop work products at the strategic and planning level?	The Contractor will be expected to provide Incident Response strategic planning, documentation, training, and associated activities.
12	Regarding training programs for Incident Response and Information Security Awareness, which COTS or HR training system is in use to host new training modules and track employee training compliance?	USAC utilizes Cornerstone Learning and Performance Suites.
13	Which roles (7.C.c, p. 14) within USAC require training content? For example, there are privileged user roles "Systems Administrators" and "DevOps Engineers", as well as standard user roles "Employee" or "System User". There are also Cybersecurity Program defined roles (e.g., CISO, Authorizing Official, ISSO, Cyber Analyst, Incident Response Lead, IT Auditor, etc.) that pertain to fulfillment of a Cybersecurity Plan functional capability. Can USAC clarify the type of role-based training for this task?	The Contractor is expected to provide Role-based Cybersecurity Training to those with privileged and/or significant information security responsibilities, which include, but is not limited to, application developers, system administrators, security engineers, etc.

Q#	Question	Answer
14	In support of FISMA audits, what IA Management system is in use to track formal IS documentation, security control implementation, overlays, architecture, roles and responsibilities, POA&Ms, ConMon plans, and so on? For example, CSAM, Xacta, eMASS, SharePoint, etc.?	USAC utilizes a combination of tools to track Information Security documentation, including Telos Xacta 360 and Atlassian Jira and Confluence.
15	How many systems (on average) require FISMA audit support?	The current average of systems requiring FISMA audit support is four (4); however, this scope may be increased to include an addition subset or all USAC systems at the discretion of the FCC OIG.
16	Are there additional audit duties in support of FISCAM or financial systems to be aware of? How many systems require FISCAM audit support?	FISCAM audit support is not scope of this solicitation.
17	Are all proposed staff to be identified with the response? Or only the individual(s) mapped to the "Security Program Consultant" LCAT? Are all additional proposed labor categories to be treated as KP as well with named individuals and resumes or is there only one KP LCAT requirement?	Offeror shall propose the Security Program Consultant at a minimum within the proposal response. While USAC does not intend to dictate the composition of the ideal team, the Offeror is expected to propose all proposed key personnel in its proposal submission. Any additional labor categories must include the experience and qualifications of the personnel to be assigned to each labor category. USAC requires that Key Personnel be assigned for the duration of the awarded Contract.
18	On average, how many Analyses of Alternatives (AoAs)/Market Research Studies are required each year?	As an estimate, the Contractor is expected to perform three (3) in-depth AoAs/Market Research Studies per contract year.
19	Does the contractor require a Facility Clearance (FCL) or do proposed staff require any level of security clearance or position of trust?	All personnel should be authorized to work within the United States. No security clearance is needed.
20	Please confirm that the contractor will not be responsible for creating the FISMA A&A packages for the systems that reside in your 5 business units.	A&A responsibilities are not in scope of this solicitation.

Q#	Question	Answer
21	Can you give us an exact number of how many systems are in each of the 5 business units and their current FISMA categorization level (L-M-H)?	Details related to systems will be provided to the Contractor after award and contract kick-off.
22	Do you have any systems currently without an Authority to Operate? If the answer is yes, how many?	Please see response to Question #21.
23	Do you anticipate running any new or planned systems through a new FISMA A&A effort during the next 12 months? If the answer is yes, how many?	Please see response to Question #20.
24	For the security program consultant key personnel slot, would you accept a substitute of 2 years of experience for candidates without a master's degree?	USAC expects the Offeror to propose key personnel, based on relevant experience and education, and associated solutions that it believes is best suited to support and meet all requirements described in the RFP.
25	Section B.6.C of the RFP mentions the Contractor should hold a kickoff meeting "no later than ten (10) workdays after any contract award." However, Section B.11.a under "Project Kick-Off Meeting" mentions that the "contractor shall initiate work" within five (5) business days. Can USAC clarify when contract kick-off will occur?	Contractor should plan to hold contract kick-off within five (5) business days after contract award.
26	Regarding the services requested in the RFP, will USAC require Offeror to utilize their own IT equipment to perform work, or does the Offeror need to use USAC owned equipment to perform work (i.e. Laptops required to perform job).	USAC will provide IT equipment to perform and deliver the work activities and deliverables described in the RFP.
27	The RFP states that work location can be performed anywhere in the U.S. given that there is a mandatory 2 day in office requirement. Will USAC consider the option of 100% remote to conduct services since travel expenses are not covered?	USAC expects personnel performing activities associated with the delivery of activities associated with this solicitation to do so physically in the USAC office at least two (2) days per week and/or present deliverables physically at the USAC office as needed.

Q#	Question	Answer
28	If hybrid work location is required, is the requirement for Key Personnel on the contract or all employees of Offeror that provide service to contract?	Please see response to Question #27.
29	Does the offeror need to fill and submit page 1 of the RFP document. If so, in which section or volume should it be included for submission?	Per RFP Page 62, the signed RFP cover page and signed Confidentiality Agreement may be submitted in PDF format as separate attachments and will not count towards the page limits for volumes 1–4 of the Offeror's proposal.
30	Please clarify, is there any set aside for this RFP?	No, this is not a federal government contract.
31	Please clarify if there is any incumbent or not?	Please see response to Question #1.
32	What is the desired timeline for the transition of activities and services to USAC personnel or a follow-on contractor? Please clarify.	Please see Deliverables #35 and #36.
33	In RFP document, on page 16, section B, heading Transition In or Out Services it is mentioned: "Provide USAC all licensing and renewal information, asset management records, software documentation, and training materials." Please clarify, are there any specific licensing and renewal processes or requirements that the contractor needs to be aware of?	USAC expects Offeror to provide reports of USAC-owned software licenses and/or equipment in use by the Offeror in support of this solicitation within the Transition Out Plan (Deliverable #36) at the end of contract period of performance.
34	In RFP document, on page 17, section B, heading 8. KEY PERSONNEL it is mentioned: ''Offeror shall provide consultant staffing for, at minimum, the labor category listed below. Offeror may also propose additional labor categories in its proposal submission.'' Please clarify how many additional labor categories can be provided?	USAC does not intend to dictate the composition of the ideal team. Offeror is expected to propose all proposed key personnel in its proposal submission. Any additional labor categories must include the experience and qualifications of the personnel to be assigned to each labor category. USAC requires that Key Personnel be assigned for the duration of the awarded Contract.
35	In RFP document, on page 61, B. Technical Capability (Volume 2), Key Personnel- it is mentioned that "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."	Please includes resumes at the end of Volume 2 (Technical Capability).

Q#	Question	Answer
	Please clarify, whether the Key Personnel should be submitted as a separate attachment or as part of the technical volume?	
38	Can we request the Government for letting us know the Level of Effort (hours per year) that is required to perform this contract.	Please see response to Question #2.
39	Page No.17, Section.8 from Solicitation document listed Security Program Consultant to be as Key Personnel. Looking at the SOW Tasks, we understand, this to be a ONE (1) FTE work. Is our understanding correct?	Please see response to Question #34.
40	Please share the incumbent company's name, and their existing contract number, and when does the current contract expire?	Please see response to Question #1.
41	Can USAC confirm if there is an incumbent for this work? If so, who is the incumbent?	Please see response to Question #1.
42	In previous advisory opportunities with USAC, offerors were required to provide recommendations for future and active procurements and to avoid a conflict of interest by not participating in such solicitations. Based on our understanding of these requirements, could USAC confirm that the vendor will only conduct market surveys to assess new solutions and COTS technologies and would not be involved in making recommendations for future procurements, and thus would be permitted to participate in future procurements?	The Offeror will not be expected to support USAC by planning for future procurements. The Offeror is expected to support and deliver AOAs and/or Market Research Studies and identify, communicate, document, and avoid any potential or actual conflict(s) of interest in carrying out those activities.
43	To allow for more accurate estimating, what level of effort is expected for the "Strategic Advisory Support" services? How many market research studies are expected per year?	Please see response to Question #18.
44	To allow for more accurate estimating, what is the expected publication date of the five year strategic plan?	Please see Deliverable #09. The Security Roadmap should be delivered no later than (NLT) one calendar year after contract award.

Q#	Question	Answer
45	Would the incident response plan development effort represent an enhancement to an existing plan, or an end-to-end overhaul / development of a new plan?	The Offeror will be expected to assess the current environment and make recommendations and provide deliverables designed to meet the requirements outlined in the RFP.
46	How many roles does USAC anticipate including in the role-based training effort and frequency of training?	Please see response to Question #13 and Deliverable #22.
47	Does USAC have an existing LMS to support role-based training, or will this be a manual build for the contractor?	Please see response to Question #12.
48	Is there a particular framework or standard(s) you would like to see applied in the development of the Information Security Program Management Plan?	No.
49	Will we be able to leverage USAC's Learning Management System to store and update training records, training requirements, and track records/reports?	Yes.
50	What is the lead time for integration with the Learning Management System?	This information will be provided to the Contractor after award and contract kick-off.
51	How many and for which specific roles will training need to be developed?	Please see response to Question #13.
52	What is the expected timeline for the annual FISMA audit? Any changes to the typical timeline we should be aware of?	Typically, the annual FISMA audit is conducted between March and August. However, this is subject to change by the FCC OIG.
53	We understand there are modernization efforts ongoing. Which of those existing or any planned IT initiatives could impact these audit processes?	None.
54	For the FISMA self-assessment, will that be FISMA Moderate or FISMA Low? Or will the self-assessment be FedRAMP Moderate or FedRAMP Low?	FISMA Moderate.

Q#	Question	Answer
55	For the FISMA self-assessment, what is the target maturity level (i.e., Level 1 – ad hoc to Level 5 – Optimized)?	Level 5 – Optimized.
56	Deliverable 01 – Annual Information Technology Risk Memo. Is this deliverable to be used as an Authority to Operate (ATO) or is it going to be used to support an ATO?	This deliverable is a stand-alone report on the state of IT from a cybersecurity perspective as well as a consolidated list of major IT risks.
57	To confirm, executing this project does not conflict the successful vendor out of conducting future Cybersecurity work for USAC, correct?	USAC cannot confirm that work on this project will not conflict with future projects. Vendor will be able to identify any possible conflicts of interest and propose mitigation plans within their proposal responses for other USAC solicitations.
58	Can the required Cover Pages per volume be excluded from page count?	As specified in the RFP on Page 62, the page limit for each volume includes the cover page.
59	Can we include a table of contents and list of graphs and tables that are outside of page count limitations?	A table of contents, graphs and/or tables are optional and will be included in the page count limits.
60	Section 7.E requires a transition plan when tasked. Given the transition plan is not a definite requirement, will USAC please confirm the pricing template can be modified to include transition services as a separately priced line item.	Offeror should include the cost of the transition plan within the specified line items on the Bid Sheet.
61	Will USAC confirm that there is an incumbent performing this work today and identify who that incumbent is?	Please see response to Question #1.
62	For consistency of evaluation across all bidders, will USAC please provide an estimated level of effort (e.g., total number of full-time equivalents [FTE])?	Please see response to Question #2.
63	Section B.11.A.a states a project kickoff meeting is required within five (5) business days, however Section B.6 (page 7) states the kickoff meeting shall be conducted no later than ten (10) workdays after contract award. Will USAC please confirm the correct timeframe for the kickoff meeting?	Please see response to Question #25.

Q#	Question	Answer
64	Section 2.3 states "Prior to delivering the Services or enabling data sharing or interoperability of any kind with USAC IT Systems, Contractor shall: (i) demonstrate Contractor system is compliant with FISMA and NIST SP 800-53 Rev. 5 and has received an Authority to Operate by the Contractor's authorizing official after following the steps laid out in the NIST risk management framework". Will USAC please confirm an ATO is required only for contractor systems that store, house, process, or transmit USAC owned data?	Confirmed.
65	Section E.1.A states 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." Will USAC please clarify to which volume potential Exceptions should be attached?	Exceptions should be clearly identified in a separate Attachment to the proposal, "Exceptions to RFP Terms" and not included with Volumes 1 – 4.
66	Section E. Past Performance states the page limitation for the overview shall not exceed one (1) page, however total page count under Section 2 states Volume 3 shall not exceed 5 pages. Will USAC confirm the total page count for Volume 3 is five (5) pages?	Offeror should provide an overview of three relevant past performance engagements within Volume 3. Each overview shall not exceed one (1) page. Volume 3 should not exceed five (5) pages.
67	"Attachment 2: Reserved" was mentioned in Section D, but wasn't included in the package. Please confirm if there is an Attachment 2 for us to complete/include as part of our response or and, if so, please provide.	There is no Attachment 2 included for this RFP; however, this attachment numbering is reserved in the event that an attachment is needed in a future revision or for the final Contract.
68	For the 5 business units with majority of these system as custom-built and on premise, are there significant changes planned for these environments within the next few years to consider?	Details related to systems will be provided to the Contractor after award and contract kick-off.
69	Will the contractor assuming the role of a CISO or to support the current CISO and the overall OCISO?	The Contractor selected will support the current CISO and the overall OCISO.

Q#	Question	Answer
70	Is the IT infrastructure (or internal network) and Information Security function centralized or decentralized for all customer-facing and business support units?	Details related to IT infrastructure, systems, and support structures will be provided to the Contractor after award and contract kick-off.
71	Does the Fund utilize an onboarding / security awareness training platform for the execution of the 'Information Security Awareness Training Support'? If not, will the contractor be responsible for providing a software solution to support security awareness training?	Please see response to Question #12.
72	How many days per week / per month would be required for on-site work for the consultant? Will the Fund be willing for the consultant to be 100% virtual?	Please see response to Question #27.
73	Does the CISO or the OCISO maintain a current Information Security Program and Strategic Plan for Information Security goals / initiatives?	Yes.
74	Does the Fund maintain a documented an Incident Response Plan?	Yes.
75	Does HR maintain an employee handbook, that includes IT Acceptable Use Rules (or IT Rules of Behavior)?	USAC has an IT Security Rules of Behavior Form that Contractor Staff must sign and mandatory IT security and privacy awareness online training that must be completed by Contractor Staff before staff may access USAC Information IT Systems.
76	Will the contractor be supported with additional staff provided by the Fund to assist in the 'Information Technology, Information Security, and Cybersecurity Audit Support' activities?	No. Offeror is expected to propose an adequate solution to meet the requirements indicated in the RFP.
77	For all services requested, is the consulting firm able to utilizes internal technical staff consultants under the direction of the senior consultant to support the Funds initiatives?	USAC does not intend to dictate the proposed staffing approach for this solicitation. The Offeror is expected to provide details regarding its proposed staffing approach in its proposal submission.

Q#	Question	Answer
78	Given the disparate activities and deliverables called for in the RFP, would USAC consider a multiple award contract, or otherwise splitting up this procurement to reduce costs and eliminate potential conflicts?	USAC intends to make a single award contract.
79	Will USAC consider a "firewall" or a proposed business process solution to mitigate OCI concerns?	Yes.
80	How many employees and contractors Cybersecurity compliance training?	Roughly 2,500 total.
81	"Provide audit support to the USAC CISO by overseeing and conduction pre-during and post-audit activities": How many audits does USAC anticipate going through on an annual basis?	Roughly three (3) audits per year, to include FISMA, A-123, and AAD audits.
82	Key Personnel Requirements: Given the disparate list of experiences and disciplines required for the Security Program Consultant Role, would USAC consider placing this expertise across multiple key personnel, instead of one?	Please see response to Question #17.
83	What is the scope of the organization/network(s) to be included in this engagement? Please provide: • Description of organization and branch offices / subsidiaries / sites? • Description of physical and cloud-based data centers? • Number of users on main corporate network? • Is the main corporate network Global? • Number of description of separate networks per site? • Any Operational Technology / Industrial Control Systems to be included in the exercise? • Size and make up of Cyber Security Team? • Size and make up of Incident Response (IR) Team? • Size and make up of other IT Teams?	Please see response to Question #70.

Q#	Question	Answer
84	Is your Cyber Security Team centrally located or is it distributed across the organization? Please elaborate if distributed.	Centrally located.
85	How would you characterize your current Information Security Program/capability? • Basic? • Intermediate? • Advanced?	Intermediate.
86	Please indicate which Information Security related documents which are available for review. • Overarching Information Security Policy/Plan? • Information Security Risk Assessment? • Business Impact Analysis document? • Privacy Impact Analysis document? • Incident Response Policy/Plan/Procedures/ SOPs/Playbooks? • Disaster Recovery Policy/Plan? • Business Continuity Policy/Plan? • Vulnerability Management Policy/Plan/Procedure? • Change Management Policy/Plan/Procedure? • Configuration Management Policy/Plan/Procedure? • Information Security Risk / Security Control Register? • Information System Security Plan(s)? • Information Security Plan of Action and Milestones (POA&M) • Cyber Security Insurance? • Other Information Security related documents?	Please see response to Question #9.
87	Is there a formal Information Security Governance Structure in place?	No.
88	Does your Organization have a Chief Information Security Officer (CISO), or any other Information Security Leadership Roles/Positions? If so, please list all Information Security	Yes, USAC has a CISO. Please see response to Question #70.

Q#	Question	Answer
	Leadership Roles/Positions, and their organizational reporting structure.	
89	Is the Senior Information Security Officer also the Senior Physical Security Officer?	No.
90	Do you adhere to any particular Information Security frameworks or standards? (NIST, CIS, ISO, COBIT, etc.)?	USAC is required to adhere to FISMA and follows the frameworks and guidance provided by NIST.
91	Do you have to any particular compliance requirements? (NIST, HIPAA, PCI-DSS, FERPA, etc.)?	Please see response to Question #90.
92	Do you operate a 24/7 Cyber Security Operations Center?	No.
93	Do you outsource any of your cyber security functions (e.g., Managed Security Service Providers)?	Details regarding cyber security functions will be provided to the Contractor after award and contract kick-off.
94	Do you have any specific objectives you'd like to achieve during this assessment?	Please see response to Question #45.
95	Do you have any other specific requests not addressed above?	N/A.
96	For the "Strategic Advisory Support," does the organization prefer one dedicated person for the scope support or can these be services using a team of consultants?	Please see response to Question #34.
97	Can the employee training program use a virtual LMS/portal or is training expected to be provided live/in person?	Please see response to Question #12.
98	How many employees will be included in the general training?	Please see response to Question #80.
99	Will role-based training be provided by department or for individual people?	The Offeror is expected to propose a solution that will allow training to individuals. Please see response to Question #13.
100	Is the contractor expected to make on-site visits for the monthly/weekly status reports?	Please see response to Question #27.

Q#	Question	Answer
101	Is USAC centralized from a security process/tool perspective (are processes uniform throughout the organization or do different departments function separately and will need to be assessed separately)?	Yes.