Universal Service Administrative Co.

Available for Public Use

Universal Service Administrative Co. (USAC)
IT-24-033 Security and Privacy Assessment Services
Questions & Answers

Q#	Question	Answer
1	Is there an incumbent and if so, what is their name and what was the previous contract amount?	USAC does not provide information regarding the incumbent and the previous/existing contract. However, multiple vendors provided services and the scope of work for this RFP is different than previous engagements.
2	Is there a pre-bid meeting?	No
3	If this is an existing project, how many assessors and Pen Testers do you currently have on the team?	USAC does not provide information regarding the incumbent and the previous/existing contract.
4	What would be the Contract Effective Date?	The estimated contract effective date is July-August 2024.
5	We would like to know if this is a brand new contract OR if there is (was) an incumbent performing these services?	See the answer to question #1.
6	If not brand new, could you please provide the current / previous contract number?	See the answer to question #1.
7	Why our firm was selected to be invited and an estimate on the number of offerors who were invited to bid?	The RFP is a full and open competition procurement. Invitations were sent to potential vendors known to perform this type of work.
8	Is there a deadline to submit questions?	Yes. Thursday, March 21, 2024, no later than 11:00 AM ET.
9	Is there a mandatory pre proposal conference for this RFP?	USAC will hold a Virtual Offerors' Conference on April 3, 2024. See RFP Section E for further instruction.
10	As regard to the bid sheet that was provided, could you list or break down the specific tasks that should be provided for "Information System and Privacy Continuous Monitoring ("ISPCM")" and "ATO"?	See RFP Section B for the full scope of services and deliverables. See also the answers to questions #98 and #99.

Q#	Question	Answer
11	Should prime contractors also include their potential sub-contractors' information as part of their bid package?	Yes.
12	Is there a maximum budget for this project?	USAC is looking for offerors to propose their best offer/cost for providing the required services as part of their proposal.
13	Is there currently an incumbent company or previous incumbent, who completed similar contract performing these services? If so - are they eligible to bid on this project and can you please provide incumbent contract number, dollar value and period of performance?	See the answer to question #1. This is a full and open competition procurement.
14	Specify the VLAN details how many is included in the Scope?	Currently, a few VLANs on premise, however the ongoing implementation of Zero Trust architecture will progressively increase segregation of networks.
15	Can you please provide current number of infrastructure details (Physical Server, Virtual Server, Network Devices, etc.)?	USAC will provide information during the Offerors' Conference
16	How much (%) of the infrastructure is in cloud?	Currently about 20% to 30% and USAC is progressively increasing cloud usage.
17	In the IT department/environment, how many employees work?	
18	Do you manage your own data Center, or do you utilize any 3rd-party/colocation facilities?	We use COLO facilities for Premise, FedRAMP CommCloud AWS, and various PaaS/SaaS FedRAMP CSPs.
19	Is there a funding/financial/budget range estimated that can help us to provide a quotation for this project?	See the answer to question #12.
20	Who is the incumbent on the contract?	See the answer to question #1.
21	What is the current level of effort in full time equivalent (FTE)?	See the answer to question #1.
22	Since USAC award information is not public, can USAC provide the current incumbent total contract value for transparency?	See the answer to question #1.
23	Are key personnel and non-key personnel required to have clearances like Public Trust prior to work on contract?	No.

Q#	Question	Answer
24	Is there any part of this engagement that must be conducted onsite? Note: RMF 4-2 & 6-2, "System Component Out-Brief Meeting" described on Page 20 indicates onsite.	No.
25	How are delays introduced by USAC in the execution of this project addressed within the contract?	Schedules are set within the first month of the base and option years. Thereafter, any adjustment in schedule is discussed and agreed about a month before the start date for any of the assessment related tasks. Ad hoc penetration testing will be requested outside the schedule.
26	Is Phishing testing expected as part of the penetration testing? If yes, can you please share the parameters USAC expects?	No.
27	Are there requirements for Insider Threat testing? If yes, can you please share the parameters USAC expects?	No.
28	When USAC uses the term RMF, are you referencing the NIST RMF 800-37 Rev 2 in the document? For example, Page 8, Section 6.A references RMF Step 4 "Assess Security and Privacy Controls". Is that RMF reference supposed to map to NIST 800-37 Rev 2 RMF steps or is that an internal reference to a USAC methodology? Step 4 in NIST 800-37R2 is "Implement" and step 5 is "Assess". Please clarify.	The RFP will be updated to reflect the steps and tasks of NIST 800-37 Rev2.
29	Does USAC provide all systems/tools for the penetration testing or does the contractor supply their own systems/tools? If USAC provides the systems/tools, please explain how that works. For example, does the contractor provide all the necessary penetration testing tools on USAC hardware that the contractor will VPN in to use?	USAC provides the Virtual Desktop Infrastructure (VDI) and will load any open source applications as agreed. If the vendor has any proprietary tools to use, then USAC will allow after review.

Q#	Question	Answer
30	How does 2.20 "Additional Requirements for Services in Contractor IT" on Page 55 apply? For this contract, is USAC requiring contractor to have FedRAMP, SOC 2, and ISO 27001 certifications?	This paragraph is boilerplate and does not apply to this contract.
31	Does #4 "Malicious Code and Malicious Cyber Activities" on Page 56 need to be adjusted due to the requirement to conduct penetration testing?	Penetration Testing is, by definition, ethical hacking that examines a system's resilience to malicious code and malicious cyber activities. As such, the Contractor will ensure that the use of malicious code or malicious cyber activities to support penetration testing are limited to the scope of the assigned test, are only executed on designated environments, and will not persist at the conclusion of any Penetration Test.
32	Since USAC is expecting the contractor to use USAC IT systems, what requirements in Section 2.10 on Page 52 are applicable?	Section 2.10 is not applicable.
33	Will all subcontractors need to be identified in the 4/10 proposal submission or can they be updated in the final statement of work if the bid is won?	All proposed subcontractors must be identified in the proposal.
34	How many Ad Hoc pen tests (Page 6) in addition to the scheduled pen tests documented on Page 22 may be required each year?	The number of PEN tests indicated on Page 22 covers both those scheduled concurrent with an Assessment and those that are Ad Hoc for the estimated 3-4 weeks of testing each. If any individual PEN test needs more or less time, then USAC will negotiate prorated cost increase or reduction.

Q#	Question	Answer
35	Do the Penetration Tests line items in Table 3 on Page 22 (highlighted below) include the pen test activities described in Tasks 1.2-2.3 starting on Page 14 for ISPCM, Focused Assessments, and ATO? Beginning in option year 2, the number of pen tests does not equal the totals for ISPCM, Focused Assessments, and ATO.	See the answer to question #34. The estimates on Page 22 are based on internal USAC system planning.
36	Will USAC stakeholders consider participating in a discovery session(s) prior to the RFP response deadline to further discuss/define the scope of this engagement, to address the above questions with the respondent and define target state goals and outcomes?	*See the answer to question #9.*
37	Is USAC interested in receiving RFP responses that include delivery approaches that are both responsive to the RFP and also outside of what was presented and requested in the RFP?	Offerors may propose creative approaches for USAC review.
38	Within what time frame does USAC expect to offer the award? Engagement kickoff is due within 5 days which will require pre-scheduling of resources.	See the answer to question #4.
39	Is there an incumbent for this work? If so, can you provide the contractor's name and any details on the size and scope of the contract?	See the answer to question #1.
40	Does USAC currently have a functioning ISPCM program, or is the intent for the successful offeror to come in and build out the program?	This RFP is for assessment and penetration testing services, not implementation of IT Security Compliance programs. USAC has an ISPCM program.
41	Does USAC currently perform annual penetration tests for the 17 FISMA systems?	Yes.
42	Does USAC currently own a suite of Penetration Testing tools? If so, can you provide a list of those tools? If not, will the successful offeror be required to purchase those licenses?	USAC will provide requested and available Open Source tools. If the selected offeror needs additional tools, USAC will negotiate to determine whether licensed by vendor or by USAC.

Q#	Question	Answer
43	Does USAC leverage a commercial GRC Platform to conduct and manage SPCA assessments?	Yes, USAC uses Telos Xacta, and the selected vendor will have specific levels of access to support assessments.
44	The Number of Systems and task activities does not match the number of systems in the Pricing Sheet. Which of the two should the pricing and proposal be based on?	Use Table 3 in the SOW and the updated Pricing Sheet. Penetration tests will be required for any system that has transitioned to Ongoing Authorization.
45	The table shows the total number of systems subject to ISPCM and focused assessment trends downward throughout the option years. At the same time, the number of penetration tests remains the same. In addition, potentially new systems will be going through the ATO process throughout the years. How does USAC plan to keep the 17 systems along with the newly ATO'ed systems compliant if the ISPCM and focused assessments are being reduced throughout the years?	USAC is implementing Ongoing Authorization (OA) and a Continuous ATO approach for systems that do not provide controls for inheritance. The penetration testing will continue to be scheduled and performed for all systems by the selected vendor.
46	What is the mix/number of systems that are on-premises versus cloud based?	See the answer to question #16
47	Are there any High Value Assets systems in the USAC inventory that require the HVA overlay of controls?	No.
48	What is the mix/numbers of Low, Moderate, and High categorized systems among the 17 systems?	All Moderate.
49	Approximately what number of "High" controls will be added for a system?	USAC has tailored our control baseline by adding currently three (3) "High" controls and removing eight (8) non-applicable "Moderate" controls that are limited to Federal entities.
50	Approximately how many "ad hoc penetration" tests" will be required on an annual basis?	See the answer to question #34.
51	What repository does USAC use for deliverables and assessment evidence?	Confluence and Xacta.
52	Does USAC use a support tool for the assessment process – e.g. CSAM, Xacta, etc..?	Xacta

Q#	Question	Answer
53	The number of systems being assessed/tested goes down after the first two years of the contract – what is to be done for the remaining systems?	See the answer to question #45
54	The estimated assessment duration for Focused Assessments does not change when the number of systems changes – should the total duration change based on the number of systems being assessed?	The estimate indicates a not to exceed and how we will use Focused Assessments to complement our transition to OA for some systems.
55	What is the mix of General Support System (GSS) and Major Application (MA) systems among the 17 systems?	One main GSS, one FedRAMP PaaS GSS supporting applications on the platform, and our common controls are assessed in a package as a system; the remainder will be MA.
56	Is there an incumbent for this work? If yes, who is the incumbent and what is their contract number?	See the answer to question #1.
57	In order scope and price the pen testing effort, approximately how many IP addresses, servers, workstations, network devices, etc. are to be pent-tested for each system?	USAC will provide information during the Offerors' Conference
58	Of the 17 systems that require penetration testing, how many are segmented networks? For example, two separate vlans with firewall rules between them that do not allow lateral movement (aka a user on vlan 1 cannot access a device on vlan 2).	See the answer to question #14.
59	If there are internal network infrastructures that have segregation, do you require segmentation testing?	Yes, once segmentation is implemented on our premise network.
60	Do any systems require Wi-Fi testing? If so, how many?	One (1)
61	Does each system's pen-test require re-testing the remediated vulnerabilities to ensure the vulnerabilities have been remediated correctly and to issue a new report?	Retesting may be requested for some remediations, and effort will be negotiated within the scope of ad hoc penetration tests. See the answer to question #34
62	Will external network penetration testing be required for any systems? If so, how many systems?	See the answers to questions #100, #209.

Q#	Question	Answer
63	Will you allow United Kingdom based penetration testers who personally hold multiple of the following certifications, OSCP, CISA, CISM, CISSP, CRT, CPSA to conduct the penetration testing from a CREST certified, ISO 27001, ISO 9001, PEN TEST approved, and Cyber Essentials Plus certified firm?	No, all services must be performed from within the United States.
64	Which FISMA security baseline (High, Moderate, Low) is selected for each system/program?	All Moderate
65	How many additional USAC-specific and Privacy controls are to be added on top of the Moderate baseline?	See the answer to question #49.
66	Do any of the systems utilize containers? If yes, which ones?	USAC will provide information during the Offerors' Conference.
67	If containers are used, are you hosting the orchestration server, or using an 'as-a-Service' tool?	USAC will provide information during the Offerors' Conference.
68	Do you have endpoint protection (Malware protection and laptop device management)?	Yes.
69	What tools are you using for endpoint protection	USAC will provide information during the Offerors' Conference.
70	What vulnerability scanning tools are in place in each environment (including contrainer scanning, as applicable)?	USAC will provide information during the Offerors' Conference. time.
71	What application scanning tools are in place in each environment?	USAC will provide information during the Offerors' Conference. time.
72	What SIEM is in place?	USAC will provide information during the Offerors' Conference.
73	Is Wi-Fi in Scope for any of these environments?	See the answer to question #60
74	Is there only one Change Advisory Board (CAB) or individual one for each system? If no, please include details.	One control board for releases and infrastructure changes. Various other processes exist for system or project change control, and architecture change planning.
75	Are any of these systems developed in-house?	Yes, about 70%.
76	For in-house developed systems, what source code repository is used?	USAC will provide information during the Offerors' Conference.

Q#	Question	Answer
77	Are USAC "Business Units" limited to the programs defined in Section 1 (High Cost, Lifeline, RHC and E-Rate) or are there additional Business Units with USAC IT systems that must be assessed?	Yes: Finance, IT for GSS, and data support systems.
78	How does USAC determine which of its IT systems must comply with FISMA?	If they hold Federal data as defined by the FCC.
79	Is there a current contractor performing assessment work on USAC's non-FISMA systems?	See the answer to question #1.
80	What criteria will be used to determine the need for a targeted assessment?	Various considerations such as need for independent assessment of some critical controls, outcome of an independent or internal audit, changes that impact limited controls, or a MA inheriting most controls with significantly fewer system or hybrid controls to assess than most other MAs.
81	Does USAC have a preferred method of transfer for assessment artifacts and deliverables?	USAC will provide access to our Confluence repository for all deliverables.
82	Does USAC have preferred templates for the briefings, memoranda, plans, and reports to be delivered?	No, as long as the essential information is comprehensive and appropriate.
83	Do all systems to be assessed have complete and current System Security Plans, including defined system boundaries, architectures, and inventory lists?	Yes.
84	Will FedRAMP packages for any cloud-based systems be promptly available for scheduled assessments?	No. The vendor may request information from a FedRAMP system package from USAC and will be provided as far as the FedRAMP CSP allows.
85	What is the distinction between focused assessments and focused penetration tests, for the purpose of this RFP?	Focused assessments are for a reduced scope of controls less than a normal continuous monitoring assessment. Focused penetration tests are for specific issue, vulnerability, finding, or component of a system.

Q#	Question	Answer
86	Can offerors combine part 7. Key Personnel with part 5. Timeline? It seems as if part 7 could be a subsection of part 5 and combing them could flow better for reviewers.	No; we need clear comparability in source selection process.
87	Can the Volume 3 page limit be increased to 5 pages or exclude the cover page due to the amount of information requested? There is a request for a description of our experience along with 3 recently completed projects (with specific details required); it would be appreciated to have at least 1 page for each (1 page for the experience description and 1 page for each of the 3 past performances).	See RFP Section E.6.E.2 for the updated page limits
88	RFP document, page 6 section 2. Type of contract. This section states the award can be single award or multiple awards based on proposed pricing line items. Please confirm offerors do not have to bid on all aspects and are able to bid on individual line items (e.g. ATO only or ATO & ISPCM only). If "a la carte" bidding is allowed, would an a la carte offeror receive less favorable ratings then offerors who bid on all 4 Attachment 1 line items?	We expect a firm fixed price for each item listed in the Pricing Sheet by year, multiplied by the number of each item, and summed by year for the FFP award. The price per year shall be the Not to Exceed (NTE) funded award. Only vendors that will provide services for all line items will be considered for award.
89	For clarification, a bidder is allowed to place a bid on only one section, i.e. (Focused Assessments)	No.
90	Would USAC be open to considering fully remote work options to attract more senior and experienced resources/staff?	Yes, with all work occurring only within the US and its territories.
91	Could you provide historical data on the number of staff/resources typically allocated to this project?	Not applicable. See the answer to question #.
92	Is there an incumbent currently in place? If there is, can you please provide the name of incumbent?	See the answer to question #1.
93	How many Full Time Employees (FTE) are currently engaged on this effort?	USAC does not provide this information. See the answer to question #1.

Q#	Question	Answer
94	How many general support systems are assessed annually and under which category will they fall per Table 3?	See the answer to question#1.
95	Will USAC furnish equipment for the contractor?	Only VDI for the penetration testing with available open source tools.
96	Since professional services organizations don't typically implement NIST 800-53 rev.5 and hold SOC2 and ISO 27001 certification, would USAC accept compliance with NIST 800-171?	See the answer to question #30.
97	Are ATOs considered full assessments? If so, are ATOs new systems being onboarded annually? If that is the case, shouldn't the number of systems to be assessed increase annually?	See the answer to question #45.
98	The "IT-24-033 Bid Sheet" does not align with Table 3 in the RFP. Please advise and clarify.	See the updated bid sheet that is aligned with the RFP Table 3, page 22.
99	The estimated quantity in "IT-24-033 Bid Sheet" doesn't match table 3 in the RFP. Can you please clarify which is correct?	See the answer to question #98.
100	What types of Penetration testing are expected to be conducted? (External Network, Internal Network, Web Application, etc.)	Primary focus is White Box OWASP penetration testing. See the answer to #209.
101	Within the "penetration testing of up to seventeen (17) USAC IT Systems" can you provide a breakdown of how many distinct applications and networks are to be tested?	In general, 1 network each and 1 to 6 applications each, average of 3 to 4.
102	Can you provide some details of the size and complexity of the applications and networks as broken out? i.e., Internal network 1 is a /16 CIDR, internal network 2 is a 4 x /8 CIDS, Application 1 is a highly complex application, etc.	USAC will provide information during the Offerors' Conference
103	What is the level of depth expected when conducting penetration tests? i.e., vulnerability scan and basic exploitation of issues to exploiting complex attack paths.	See the answer to question #100
104	Since cloud assessments and review of cloud systems may be required, should the vendor be a FedRAMP 3PAO?	No.

Q#	Question	Answer
105	Does the awarded organization need to maintain ISO 9001:2015 certification to ensure quality of deliverables?	No.
106	Will USAC provide guidance on invoicing? Is the expectation that the contractor will invoice monthly based on each unit (assessment or pen test) completed monthly? Or is USAC expecting a fixed amount every month?	Contractor will invoice at conclusion of and USAC's acceptance of each assessment or penetration test final deliverables.
107	The RFP states, "If Offeror currently has staff or personnel who meet the qualifications for the services identified in Section B.7 and Section B.8 who are available for assignment under an awarded contract, please provide a resume (not to exceed two (2) pages per resume) that includes their educational background, specific job and related experience, and the specific position(s) for which they are available on the Contract." Are resumes for staff other than those designated as Key Personnel required to be submitted with the proposal?	No, only Key Personnel need provided resumes.
108	If USAC sends a past performance questionnaire to the contacts identified in an offeror's proposal, how will USAC notify the offeror the questionnaire was sent (i.e., will the offeror be "CC'd" on the email containing the questionnaire, notified via a separate email, or notified by another means?) so that offerors can follow-up with contacts to ensure a response back to USAC?	USAC will notify the offeror via a sperate email if USAC determines that it is needed. Offerors must ensure their proposed references respond to USAC questionnaire.
109	The RFP states, "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." Could USAC please confirm a .PDF file type is acceptable for the file submission of each proposal volume?	Yes.

Q#	Question	Answer
110	Would USAC please consider omitting the Cover Page from the page limits for Volume I, III, and IV?	See RFP Section E.6.E.2 for the updated page limits. Cover page is still included in the page limit.
111	Could USAC confirm that Table of Contents are not included in page counts for any volume?	USAC does not require table of contents. If offerors wish to include table of contents, they must be included in the page count as updated. Procurement will answer this question.
112	The RFP states USAC will make a responsibility determination considering whether the Offeror has the accounting systems, internal controls, quality assurance processes and organizational structure and experience necessary to assure that contract work will be properly performed and accurately invoiced. We recommend information about Offerors' accounting systems, internal controls, quality assurance processes and organizational structure should be provided in Volume I – Corporate Information and respectfully request USAC allow 5 additional pages within the page limit to ensure each of these areas can be addressed sufficiently so that USAC can make a responsibility determination.	See the updated page limit. USAC does not require this information now. Offerors may decide to include a summary of these information in volume 1 if they wish to. USAC will ask for detailed information later if needed.
113	Is this work currently being performed by a contractor and can USAC name the current service provider(s)?	See the answer to question #1.
114	If this is current work, are there any transition-in activities that will need to be performed by the eventual awardee?	Yes, however, not beyond the description of work and deliverables during the first month of the contract.

Q#	Question	Answer
115	The instructions for Technical Capability (Volume II) mentions the volume must include "2. A summary detailing Offeror's experience providing security and privacy control assessments in the capacity described in Section B of this RFP." Because this is already being addressed as part of Volume II, Section 6 - "Experience", and further detailed in Volume III Past Performance Information, would USAC consider removing this requirement from Volume II?	Volume III Past Performance Information requires specific information about your most recent projects while volume II requires a summary of your relevant experience. This will remain unchanged.
116	After Task 1.3 within the Scope of Services section (Page 16), the document includes a bolded title that reads "4. Reports." Can USAC confirm that the requirements and deliverables associated with this task are to be included as part of Task 1.3 Security and Privacy Assessment Report?	All requirements and deliverables associated with "4. Reports" section are delivered for each assessment along with "3. RMF Step 4.3 (TASK 1.3) – Security and Privacy Assessment Report" section.
117	USAC mentions that "Assessments shall be in accordance with the NIST RMF, NIST SP 800-37 Rev 2." However, the listed RMF process steps (e.g., RMF Step 4-1, RMF Step 4-2, etc.) do not exist within the Rev 2 guidance. Can USAC please clarify if the listed RMF Steps are accurate?	See the answer to question #28
118	Will USAC please clarify the intent and expectation of "focused assessments"?	See the answers to questions #45, #54, #85.
119	On average, per year, how many ad-hoc penetration tests, focused assessments, and focused risk assessments have occurred?	See the answer to question #34.
120	Please confirm email address for quote submission, hyperlink on this page is linked to rfp@usac.org.	Procurement@usac.org and Mustafa.Kamal@usac.org
121	Is there an incumbent contractor performing this work? If so, please provide the name and contract number.	See the answer to question #1.
122	Please elaborate on the complexity of the systems (i.e. average number of devices)?	See the answer to question #15

Q#	Question	Answer
123	The number of systems listed in Table 3 does not align with the number of systems identified in the Bid Sheet. Please explain the variance.	See the answer to question #98.
124	Does the estimated assessment duration include reporting deliverables as well?	For those reporting deliverables associated with each assessment.
125	How does USAC define "focused assessment"	See the answers to questions #45, #54, #85,
126	How does USAC define "ATO assessment"?	See RFP – any full assessment of a system anticipating a recommendation for authorization.
127	Are table of content pages included in the overall page limit for each volume?	See the answer to question #111.
128	Can USAC confirm that it is requested for the offeror to discuss "experience" in Volume II and Volume III? If this is the request, can the offeror refer between the two volumes in order to maximize utilization of page limitations?	See the answer to question #115.
129	How many of the existing systems are on premises vs on cloud?	See the answers to questions #16, #75
130	USAC FISMA systems will need to be reauthorized not only every 3 years but whenever there is a significant change to the system. For ex. Moving from On-Premises to Cloud. Does table 3 factor in these upcoming significant changes when listing 2 ATOs each year?	Depending on the Security Impact Analysis (SIA) for the change, a reauthorization would usually require an ATO level assessment, included in the estimates for ATO in Table 3.
131	Can you please clarify how companies will be evaluated, if not on price? Will a large business with more geographical locations with a higher price be evaluated higher over a small business with fewer geographical locations that offers a lower FFP proposed cost? "A company, its name-recognition, geographical offerings, and the expertise/experience of staff impacts the price of the services offered by the firms, thus making comparisons of differently situated firms less meaningful."	This is a full and open competition. USAC will evaluate all offerors based on evaluation factors included in RFP Section E. See updated Section E. 7. C.

Q#	Question	Answer
132	On Page 59 of the RFP, it states that "proposals must be submitted in the form of one (1) electronic copy submitted to procurement@usac.org." However, on Page 61 of the RFP, it states that "proposals shall be presented in four (4) separate volumes." Can the Government kindly confirm the number of volumes that are required for submission?	Proposal should be presented and submitted in four separate volumes.
133	Is there any incumbent on this contract, if there is any, what is the contract number and name or is it a new requirement and level of effort?	See the answer to question #1.
134	Can the government please share the labor categories (excluding the Project Manager, Lead Assessor, and Penetration Test Lead)	N/A – USAC is a non-governmental entity. See the answer to question #1.
135	Can the government please confirm on required level of effort (total estimated hours per year)?	No –USAC does not provide this information.
136	Can the Government please confirm in which volume entire first page of RFP the (CONTACT INFORMATION) is to be submitted?	The RFP cover page can be submitted as separate document.
137	Regarding page 1 of the RFP, would USAC please clarify if the completed contact information page [and signature block] is required with proposal submission? If so, where should offerors insert this page?	Yes, this is required with proposal submission and can be submitted as separate document.
138	On page 59 of the RFP (Section E.1.B), would USAC please confirm if all four (4) volumes should be submitted in one (1) electronic file?	See the answer to question #132.
139	On page 61 of the RFP (Section E.5), would USAC please clarify if there's a length requirement for the volume cover pages?	Yes, it should be one page.
140	On pages 61-62 of the RFP (Section E.6.A.4), if no actual, potential, or apparent conflict of interest exists, are offerors still expected to submit a mitigation plan in Volume I?	No.

Q#	Question	Answer
141	On page 63 of the RFP (Section E.6.B.6), would USAC please consider removing the "Experience" requirement from Volume II as it will already be addressed in Volume III?	See the answer to question #115.
142	On page 65 of the RFP (Section E.6.E.2.c), would USAC please consider increasing the page limitation for Volume III from 4 pages to 5 pages?	See RFP Section E.6.E.2 for the updated page limits. .
143	On pages 69-71 of the RFP (Attachment 2), would USAC please clarify if the signed confidentiality agreement is required with proposal submission? If so, where should offerors insert this page?	Yes, it can be submitted as a separate document/attachment to the proposal
144	Is there an approved budget for this activity that can be shared with KUMA?	USAC does not provide this information.
145	Does USAC have current security certifications (3rd Party)?	Not applicable.
146	1 year contract with 4- 1-year renewable options - What would cause a change in the options? Is there anything that would take an option off the table?	This is USAC's standard contract term. Option years will be exercised based on USACs discretion.
147	Will USAC give access to your IT Systems for USAC documentation storage? SharePoint access or other?	See the answers to questions #51, #81
148	How many web-based apps? In how many states?	USAC will provide information during the Offerors' Conference
149	How many API's and web-based apps?	USAC will provide information during the Offerors' Conference
150	USAC IT Systems - can we get a definition of each system?	See the answer to question #55; each SSP will provide definition of each system.
151	USAC IT Systems - can we get mappings/diagrams of each system?	See the answer to question #55; each SSP will provide diagrams of the systems
152	USAC mission systems are deployed on On-Premises and Cloud-Based infrastructures. Which cloud-based infrastructure(s) is/are the vendor working with?	AWS primarily, Azure for some SaaS, OCI, and Accenture Cloud. We also have systems operating on PaaS and SaaS FedRAMP offerings.

Q#	Question	Answer
153	USAC mission systems are deployed on On-Premises and Cloud-Based infrastructures. Has the system been through any third party audits? If so, which ones? When was the latest?	All USAC authorized systems to be assessed under the scope of this RFP have been assessed by an independent third-party assessor.
154	The planned number and type of assessments and penetration tests for the base year and each option year. 11 systems to test at 5-6 weeks each -the math goes beyond the 1 year scope - is there room for expanded time? Can we test in parallel? Any dependencies?	Reference the paragraph at "Table 3" addressing the minimum level of concurrent performance of assessments and penetration tests required.
155	Contract Term - Is the project end date one year after the effective date?	The contract term is one base year with four 1-year renewable options.
156	Lessons Learned-the list of individuals - The list in the notes - is this the list of USAC Stakeholders? Any stakeholders missing?	These are the primary stakeholders that USAC considers essential for adequate coverage of the task. There may be additional stakeholders identified by the USAC ISSO.
157	What do the Notices/Consents/Approval list mean?	Anything that would alter or legally enforce the terms of the USAC Standard Terms and Conditions such as contract termination or revision to the USAC Standard Terms and Conditions
158	Added Services - what defines added services?	This would be a change request from USAC to the contract extending the scope of the contract or additional services.
159	PII - 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. Is there a USAC template log? Does KUMA maintain this log?	The penetration testing or an evidence artifact may inadvertently include or expose PII. USAC will conduct incident management in accordance with the identified NIST and OMB guidance should such an event occur.
160	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 - Is FedRAMP authorized certification a hard requirement?	No. See the answer to question #30. Also, paragraph 2.10 is boilerplate, not applicable to this contract.

Q#	Question	Answer
161	2.17 - Security and Privacy Assessments-Is it a hard requirement that the vendor be FISMA certified?	2.17 is boilerplate, not applicable to this contract.
162	2.17 - Quarterly representations to USAC any changes to controls/procedures - Is this starting in Y1 or after Y1?	2.17 is boilerplate, not applicable to this contract.
163	ISO 27001 certification - Is this a hard requirement?	No. See the answer to question #30.
164	SOC 2 Type II report - Is this a hard requirement?	No. See the answer to question #30.
165	FISMA compliance - Is this a hard requirement?	No. See the answer to question #30.
166	Standard Information Gathering Lite documentation - Does USAC have an existing template? Is this a hard requirement?	No. See the answer to question #30.
167	Can we include a subcontractor on our Team for the delivery of the scope? If yes, can we include the work of a subcontractor as a Past Performance in Past Performance Information (Volume III)	Offerors may propose subcontractors. The proposed scope and engagement of the subcontractor must be identified in the proposal. Offeror may include the work of a subcontractor as a Past Performance in Past Performance Information (Volume III)
168	Can we add a Table of contents to all the volumes and please confirm whether it will be counted in the page limit?	See the answer to question #111.
169	Where are the up to 17 systems to be assessed hosted? Are there controls inherited from the hosted provider?	The main GSS, any FedRAMP CSP, and the common controls provide a large set of inherited controls for Major Applications.
170	How often are updates and enhancements to the 17 systems performed?	Continuous monitoring assessments are annual. Updates and enhancements are frequent for all systems.
171	What is the frequency that the systems are assessed? Annually? Quarterly? Is there a desire to move towards a continual assessment process?	See the answers to questions #170, #44, #45.
172	What tools are in place today to support the assessment and pen testing? Can the contractor bring in tools to optimize and enhance assessments and pen testing?	See the answers to questions # 29, #42, #95.
173	What is the incumbent contract number?	See the answer to question #1.
174	If there is an incumbent contract, who is it awarded to presently?	See the answer to question #1.

Q#	Question	Answer
175	If this is an existing contract, how many FTE are currently staffed on the program?	USAC does not provide information regarding existing contract or incumbent.
176	What tool stack does USAC use? An optimal approach would leverage tools that USAC has already paid for and invested in.	See the answers to questions # 29, #42, #95.
177	What small business goals are associated with this procurement?	This is a full and open competition procurement.
178	If there are small business goals, what categories need to be met?	This is a full and open competition procurement.
179	Are there other external agencies assisting in the security assessment process? Any leadership stakeholders outside of USAC?	No.
180	Table 3, page 22 – refers to estimated tasks per year. Does this the current count of tasks, or aspirational?	As the table name indicates, it is the estimated number based on current scope of systems at USAC.
181	What other security considerations are given outside of OMB, NIST, FIPS, and USAC security? NARA?	We do comply with NARA and are subject to Binding Operational Directives, and Presidential Orders and Memoranda when directed by FCC.
182	Is there another contractor functioning as an outside assessor? If so, who is that contractor?	No.
183	How soon after the written request must the Contractor provide current versions of the requested documents?	See the answer to question #30.
184	On the cover page, the offeror's statements verifying that the proposal is valid for 120 days - Is that from the submission day (April 10, 2024)?	Yes
185	To what volume should the signed Confidentiality Agreement be attached?	This can be attached/included as a separate document to the proposal.
186	Does the confidentiality agreement count against the page count? If so, would you please consider excluding it from the page count?	No.
187	Does the cover page count against the page count? If so, would you please consider excluding it from the page count?	No.
188	Does the table of contents count against the page count? If so, would you please consider excluding it from the page count?	See the answer to question #111.

Q#	Question	Answer
189	Can you please provide the dollar value of the incumbent contract? We understand the scope was smaller, but it would help us better understand the current level of effort	See the answer to question #1.
190	Can USAC please clarify how many IT systems are deemed to be in-scope? If 1/3 of the controls are required to be tested annually, how does the number of systems on page 22 (Table 3) breakdown for the multiple years?	All authorized systems are assessed on a base set of key controls, about 50% of the controls list, plus about 1/3 of the remaining controls that rotates each year so that 100% of the non-base controls are covered every 3 years.
191	Can USAC please clarify how many IP addresses are requested to be scanned as part of vulnerability testing?	USAC will provide information during the Offerors' Conference
192	With the understanding that each business unit uses one (1) or more IT systems, can USAC please briefly describe what IT/cyber/privacy components are managed centrally or in a decentralized manner?	USAC will provide information during the Offerors' Conference.
193	CAN USAC please clarify approximately how many of the following are in scope for the penetration testing (as applicable) for a sample year: 1. Desktop/laptops 2. Servers 3. Databases 4. Routers and switches 5. Publicly available IP addresses 6. Internally reachable IP addresses 7. Physical locations 8. Number of remote employees 9. Number of wireless access points	USAC will provide information during the Offerors' Conference.

Q#	Question	Answer
194	Last year's FISMA report indicates there are 25 improvements recommended in Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, and Information Security Continuous Monitoring. Can USAC please clarify if there are any IT projects or initiatives for this year or in the near future that could impact the scope (i.e. system migrations)?	USAC cannot provide this information at this time.
195	Does USAC have their own approved vulnerability scanning tool that should be leveraged or will USAC need to leverage the contractor's vulnerability tools?	USAC will provide information during the Offerors' Conference. .
196	What is the maximum number of past performances allowed from the subcontractor?	USAC does not specify this requirement.
197	Who is the incumbent on this project?	See the answer to question #1.
198	The RMF steps in the scope of services and deliverables do not match up with the most current RMF V2 publication. Would USAC wants vendor to follow the most current RMF steps or the ones in the RFP?	See the answer to question #28
199	"All Assessors must have CISA/CISSP/CAP/GSNA". Does the Assessment project manager (ASP) need to have one of the certifications mentioned for all assessors or can the ASP have a sperate certification?	The term in the RFP is Assessment Project Manager (APM) and a different certification is acceptable.
200	"Contractor shall assign, as Key Personnel, at least one (1) each for the Assessment Project Manager, Lead Assessor, and Penetration Test Lead, and assigned Staff." Can Key Personnel for PM, Lead Assessor, and Pent Test Lead be the same person?	USAC requires the offeror to perform up to three concurrent assessments and two concurrent penetration tests. As such, any of the three (3) Key Personnel required may also work as an Assessor Staff or Penetration Test Staff.

Q#	Question	Answer
201	Would USAC please confirm whether the current tasks in this section are currently performed by another company? If so, would USAC please share the name of the incumbent and the current contract value of the award?	See the answer to question #1.
202	Would USAC please confirm whether there are any security clearance requirements for key personnel or team members?	There are no security clearance requirements.
203	Would USAC please confirm whether it will require all team members to participate in the hybrid schedule, or is USAC asking for a team representative to be on site on the respective hybrid days?	This contract will allow primarily remote contract execution with on-site attendance as an exception when requested.
204	Would USAC please confirm whether it currently uses a Governance, Risk, and Compliance (GRC) application to track and store all IT assessment and systems' documentation (i.e., System Security and Privacy Plan, Privacy Impact Assessment)? If so, would USAC please provide the GRC application name?	See the answer to question #43
205	Would USAC please confirm whether virtual sessions will meet the requirement for Direct Observation?	Yes.
206	Would USAC please clarify that paragraph 7 allows for revised frameworks, standards, and other guidance that supersedes the publications referenced in paragraph 6 (NIST SP 800-37 Revision 2, Appendix A)?	Yes.
207	Would USAC please confirm that this is System Owner (SO) memorandum entrance memo written for all SO stakeholders?	Yes, as entrance of the system into assessment.
208	Would USAC be amenable with reviewing assessment tools that could be configured to meet these requirements (e.g., DHS CISA CSET Tool) while providing analysis?	Yes.

Q#	Question	Answer
209	Would USAC please confirm that it will provide authenticated vulnerability scanning tools and results or if the contractor will be required to utilize their own equipment and tools? Would USAC please confirm whether the penetration testing will be performed from the internal network or if external testing is being requested?	USAC will provide vulnerability scanning tool results. Penetration testing is primarily from internal network; however some external testing of web apps may be required.
210	Would USAC please confirm that graphics, headers, footers, and footnotes may also be less than 12-pt font, in addition to diagrams, tables, and charts?	Yes, but they must be readable.