RFP IT-19-086
CISO Advisory Services
Questions and Answers

#	RFP Reference	Question	Answer
1	N/A	Is this a new requirement or is there an existing incumbent? If an incumbent is providing support, how big is the team?	This is a new requirement.
2	N/A	Is this requirement being set-aside for a Small Business?	This is not being set-aside for small business.
3	N/A	The RFP provides no information to assist the offeror in determining the level of effort to be applied. It is critical to understand what USAC seeks to accomplish in this three-year contract for the CISO Advisory and Support services, preferably on a year-by-year basis.	This RFP is for advisory services specific to overall security program management. This role consists of an individual contributor for one base year and up to two option years.
4	N/A	Does USAC have a Governance, Risk and Compliance (GRC) tool (i.e., Xacta; CSAM, etc) implemented? If not, where is security documentation/artifacts stored?	Xacta has been installed as of Dec. 2019
5	N/A	How many contractor teams support the USAC's Information Security Program (i.e., ISSO, Security Control Assessor, Security Operations Center teams)? What are their roles and how big are each teams?	Currently there are 2 contractor teams. One provides Assessment and Authorization (A&A) and the other Security Controls Assessor (SCA) support.
6	N/A	Is the USAC Chief Executive Officer ("CEO") or the Chief Information Officer ("CIO") the authorizing official for USAC systems under the NIST RMF?	CIO
7	N/A	Attachment 2 (Invoice Schedule) seems be missing or is this a template that the Vendor has to create. If the Vendor has to create this, what is the suggested format?	Attachment 2 invoice schedule must be submitted by the vendor. There is no template.
8	N/A	Attachment 3 (Confidentiality Agreement) is missing	Attachment 3 has been posted to the USAC website.
9	N/A	Does USAC want or require a Table of Contents for each volume?	A table of contents is not required. If a table of contents is submitted, the vendor must include it in its page count.
10	N/A	What is the font type/size required? Should text be single-spaced?	The is no formatting requirement. The proposal must be legible.
11	Section B.IV	Please clarify place of performance – It is stated that all required contract services must be performed at USAC headquarters then later states that Status and other meetings may be held telephonically or in person, at USAC's discretion. USAC will not reimburse Contractor for any travel related expenses for kick-off, status, and other meetings. Is there work that can be done remotely or certain personnel who can be remote? If remote is allowed, is this on a case-by-case basis as situations arise, or can some / all personnel be remote permanently?	All work must be performed at USAC headquarters.
12	Section B.I., paragraph 2	Which NIST framework does USAC use; Risk Management Framework (RMF) or Cybersecurity Framework (CSF) or both?	RMF Framework

13	Section B.I.	Are any systems managed in a FedRAMP cloud environments?	Yes; however, those systems are managed by third party vendors.
14	Section B.VI.A.1	Which USAC Information Security Program domains are currently mapped out?	USAS has the following domains: 1. Security Risk Management, 2. IAM, 3. SOC/Sec Engineering, 4. Compliance, 5. Business Continuity, 6. Application Security, 7. Physical Security, etc.
15	Section B.VI.A.1.i.a	Which NIST framework; Risk Management Framework (RMF) or Cybersecurity Framework (CSF) or both?	RMF Framework
16	Section B.VI.A.1.iii	Does USAC currently have a IT Contingency Plan including Testing and Exercises?	Yes
17	Section B.VI.A.1.iii	Does USAC currently have an Incident Response Plan including Testing and Exercises?	Yes
18	Section B.VI.A.1.iii	Disaster Recovery wasn't a part of developing monthly metrics? Is this requirement? If so, does USAC currently have a Disaster Recovery Plan including Testing and Exercises?	USAC does have a Disaster Recovery Plan. This is not part of the monthly metrics.
19	Section B.VI.A.1.iii	For the information security education, training and awareness metrics development, is there a Learning Machine System (LMS) or some other tool/mechanism used to track training requirements to support developing monthly metrics?	Yes
20	Section B.VI.A.1.iii	Will the contractor be responsible for managing the USAC security awareness program and providing the training curriculum for the training?	Yes
21	Section B.VI.A.2.ii	The requirement is to manage internal and external-facing SharePoint sites. Please state whether this is simply managing the content or if significant SharePoint development/configuration is required. This is necessary to understand whether a knowledgeable SharePoint developer is required.	Managing the content only
22	Section B.VI.A.2.ii	What version of SharePoint being used that the external customers use?	The Extranet is on WSS 3.0 also known as SharePoint 2007. The server hosting it is Windows Server 2003.
23	Section B.VI.A.3	Does USAC currently have an existing information security education, training and awareness program in place? Is there a Learning Machine System (LMS) or some other tool/mechanism used to track training requirements?	USAC currently has an existing IS education, training and awareness program. There is a LMS to track requirements.
24	Section B.VI.A.4.V	Which team as part of the USAC Information Security Program will the contractor work with to ensure NIST privacy controls are documented, as required, for each USAC information system?	The A&A vendor.
25	Section B.VI.A.4.vi	How many PTA's and PIA's are anticipated in a year?	PTA's and PIAs are needed for each system. There are currently 8.
26	Section B.VI.A.4.vii	It mentions "Manage and maintain a process for reporting policy violations." Are the policy violations, privacy violations or some other violation?	Privacy violations.

27	Section B.VI.A.5	When was the last FISMA system Audit?	USAC's GSS and EDS systems.
28	Section B.VI.A.5	Will the contractor be responsible for supporting any other compliance audits in addition to FISMA? For example, A-123, FISCAM, GAO, OIG, or SOX audits? See page 11, Section E. Audit Support Services, subsection i.	Yes. DMF audit and other audits upon request
29	Section B.VI.A.6	Does USAC have their own vulnerability scan toolset? If so, what vulnerability scan tools are they?	Yes. USAC uses Tenable
30	Section B.VII.B	Are there any mandatory or minimum certifications that the Security Program Consultant key personnel position must have?	There are no mandatory certifications. The RFP has been updated to include a list of preferred certifications.
31	Section B.VII.B	Is the vendor responsible for performing vulnerability assessments? The following is stated: Review vulnerability scan results to perform vulnerability assessment	Vulnerability/Scanning Management Support has been removed from the scope of this RFP.
32	Section E.V.B.7.a	Are resumes required for any other personnel that will be assigned to USAC and his/her role on the contract (non-key labor category) proposed?	Resumes other than key personnel are not required.
33	Page 4, Section B.I: Overview Page 6-10, Section B.VI: Scope of the Services and Deliverables	Section B.I: Overview and Section B.VI: Scope of the Services and Deliverables do not align (Privacy Support and Vulnerability/Scanning Management Support are missing). Can USAC please confirm the scope of services will include Privacy Support and **will not include** Vulnerability/Scanning Management Support?	Vulnerability Scanning Management will not be a part of the scope of this proposal.
34	Page 33, Section E.V.B: Technical (Volume II)	Please confirm that Attachment B: “Exceptions to RFP Terms” for Volume II: Technical is **excluded** from this volume’s page count limit.	Attachment B: "Exceptions to RFP Terms" is excluded from the page count limit.

35	Page 36, Section E.V.D.3: Attachment 2 Invoice Schedule Page 10, Section B.VII.A.d	Can USAC clarify the expectation and differences of the milestones and deliverables in the Invoice Schedule from the Project Plan that is to be developed over the scope of this work as defined in section B.VII.A.d? Is the intent of the Invoice Schedule to solely identify when USAC should expect invoices to be received and due date?	Because this is a firm fixed price contract, the invoice schedule will define specific dates for issuing invoices for corresponding milestones and deliverables.
36	Page 36, Section E.V.E.2: Page Count Limits	Please confirm that tables of contents for Volumes I to III are **excluded** from each volu	Table of contents are not required and are included in the page count limits.
37	Page 36, Section E.V.D: Price (Volume IV) Page 36, Section E.V.E.4: Page Count Limits	As written, Volume IV would require a minimum of 3 pages. Please confirm that USAC will the page count for Volume IV to read "may not exceed three (3) pages, including Cover page, Attachment 1, and Attachment 2.	Attachment 1 and Attachment 2 are excluded from the page count limit.
38	Page 38, Section E.VI.C: Responsibility Determination	To be compliant with VI.C - Reasonability Determination, can USAC confirm that all Offerors must have an accounting system that accumulates and segregates direct from indirect costs and/or meets compliance with DCAA, CAS, and/or FAR requirements within the last 12 months?	Offerors must be able to submit accurate invoices in accordance with the terms and conditions of this contract.
39	N/A	Will USAC permit work to be done at the contractor's location?	All work must be done at USAC headquarters.
40	N/A	Will USAC be amenable to substituting educational experience for work experience?	Yes

41	N/A	Will USAC consider separating the key personnel (Security Manager) role into multiple roles?	No
42	N/A	Is this RFP designed to obtain a single person/role to act as a CISO or is USAC expecting to implement a team of personnel to perform in the CISO support role?	This RFP is designed to obtain a single person to support the USAC CISO.
43	N/A	Is there an incumbent on this contract?	There is no incumbent.
44	N/A	Will USAC provide a contract ceiling amount?	USAC will not provide a contract ceiling amount at this time.
45	N/A	Does USAC have an anticipated level of effort for resources?	No
46	N/A	Have the systems in scope of this contract gone through the ATO process?	Yes
47	N/A	Is there any current information security program in place or is this contract to stand up a security framework and risk management program?	A security framework and risk management program is in place but needs to be modified/improved.
48	N/A	Will a USAC security team execute the framework the CISO puts in place, or will the contractor be responsible for executing the framework (i.e., will there be USAC staff or additional contractors from other contract vehicles to support things like assessments, continuous monitoring, documentation packages, etc.)?	There will be USAC staff and contractors to support the execution of the proposed framework.
49	N/A	Is there a USAC team to support this contract?	Yes.
50	P.35 - C.2.B	Will USAC be sending past performance questionnaires?	USAC will be emailing past performance questionaires to the points of contacts listed in Volume III.
51	Section B.VI.A.6.ii	Should the Vulnerability/Scanning Management Support task follow the NIST SP 800-115 guidelines?	This no longer applies to this proposal. Refer to answer 33.
52	Section B.VI.A.6.ii	Is it the expectation that the Vendor will be performing vulnerability assessments and not vulnerability scans?	No. This no longer applies to this proposal. Refer to answer 33.
53	Section B.VII.B	Where do we put the support for "Any additional labor categories must include the associated labor hour bill rate for each additional category submitted as well as the experience and qualifications of the personnel to be assigned to that labor category." Can there be an Appendix?	If you are proposing additional key personnel outside of what is listed in the RFP, include the resume in Attachment 4 (Resumes) to Volume II.