Universal Service Administrative Company (USAC)
USAC IT Security Operations Center – IT-23-064
Questions & Answers

Q#	Question	Answer
1	This appears to be a selection process for only existing USAC contractors either as the incumbent now or with specific experience working with USAC based on this requirement "Contractor must have a proven track record of embedding resources into an already existing and maturing USAC Security Operations team" Will USAC consider other contractors that specifically have experience with Splunk, all of the stated tools and have current past performance? Will this requirement be removed?	In review of the language in question, USAC has posted a revised RFP with an update to this sentence that states "Contractor must have a proven track record of embedding resources into an already existing and maturing team of similar size and scope to the USAC Security Operations team." The selection process is open to all qualified vendors regardless of their experience with USAC.
2	Who is the incumbent now and are they intending to bid on this work?	There is not a current incumbent contract for these services. Normally, USAC does not provide information regarding incumbent contractors.
3	Can you please describe your Splunk environment. For instance- Do you have Splunk core? Enterprise Security, Phantom, etc. Which licenses do you currently hold - what are their timeframes - will you need help w license acquisition? What type licenses - perpetual - term - Cloud - on prem What are the size of the license (For instance - how many GB or SVC's are the license sizes)	Splunk Cloud in GovCloud, 500 GB ingestion. Includes dedicated ES, IDM, and SHC. On-prem HF, UFs, and DS to manage.
4	Are you asking for full service Splunk and MSSP/SOC Services?	Partially, expecting managing Splunk Cloud engineering with SOC services. No other managed security services are required.
5	Which EDR are you currently using, and would you like managed EDR services ?	USAC is currently using Carbon Black and will continue to manage other security tools. Managed EDR services are not needed.

Q#	Question	Answer
6	"The purpose of this RFP is to acquire professional services for 24/7/365 managed services and monitoring of USAC's Splunk Cloud and Splunk enterprise security environment. This includes alert triage and tier 1 incident response.", There seems to be a contradiction between Section 2 and Section D Accessibility as the scope of this solicitation requires 24/7/365 environment while as in section D, the working hours are given between 09:00 AM to 06:00 PM. Can USAC clarify whether Key personnel are required on call basis during the weekends or on emergency basis?	Working hours are for USAC FTE Incident leaders and Splunk managed services. SOC monitoring will need to be 24/7/365.
7	Referring Section F Key Personnel, "USAC's understanding is that a team of 2-3 full time Contract Personnel per shift will provide the needed level of effort", since this is 24/7/365 environment, can USAC confirm the number of hours per shift?	8 hours
8	Referring to Section B.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." We understand that proposed Personnel mean SOC Analysts. Can USAC clarify what they expect from other Personnel assigned to USAC?	USAC expects Splunk engineering roles as well as leads/proposed project leads.

Q#	Question	Answer
9	Referring to Section B.4.b Key Personnel," 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." What exactly is USAC expecting to provide?	If any proposed key personnel are known to have an upcoming separation date from the Offeror's company but are expected to complete work on the Contract prior to this separate date, the key personnel and their anticipated termination date must be identified in the Offeror's proposal to the RFP. The personnel that will replace the separated key personnel should also be identified, if possible.
10	Will USAC consider multiple pricing offers for these MSSP services; i.e month-to-month or yearly upfront payments?	The submitted Price Proposal should be based on FFP and T&M pricing with a total NTE ceiling price indicated in a completed Bid Sheet (Attachment 1).
11	What is the thought process behind an expectation of 2-3 dedicated resources per shift? Could you please explain where this expectation comes from and what factors play into this?	8 hour shifts to support 24/7 monitoring.
12	Could you share the size of the Splunk environment? Please share any details that would help us understand the level of effort that our resources would be expected to manage.	Please see answer to Question 3.
13	Does USAC have an expected budget for this procurement?	USAC does not provide this information. Offeror should provide its best estimate based on the scope of work stated in the RFP.
14	Would USAC accept proposed key personnel with industry certifications from organizations such as GIAC, EC-Council, or ISC2 in lieu of the requested CySA+ or Splunk Fundamentals certifications?	Yes. USAC's expectations are to have Security trained professionals. The Certifications listed are an example; other certifications will be accepted.
15	How is this solicitation related to TORP 23 IT Security Operations Services USAC-20-015 released last year?	RFP IT-23-064 is a revised solicitation of the TORP/RFP that was released last year.

Q#	Question	Answer
16	Would USAC consider substituting CompTIA Secure Infrastructure Specialist (CSIS) - which stacks CompTIA A+, CompTIA Network+ and CompTIA Security+ - for CYSA+?	Please see answer to Question 14.
17	Would USAC consider substituting one or more of these Splunk certifications in lieu of Splunk Fundamentals 1, 2 and 3 for the PM key personnel requirement? Splunk Enterprise Certified Architect, Splunk Enterprise Certified Administrator, Splunk Core Certified Power User, Splunk Core Certified User	Please see answer to Question 14.
18	Is there any incumbent contractor working on this project?	Please see answer to Question 2.
19	Can USAC please provide historic data of estimated tickets for SOC support?	Roughly 300/week medium and above alerts requiring investigation. Average is 2 incident escalations per month. Roughly 50 engineering tickets for false positive remediation per month.
20	How many incidents does USAC anticipate every month?	Based off USAC's history, we anticipate two defined security incidents per month.
21	Can USAC please provide historic data for SOC incidents?	Some examples include data exfiltration (corporation with internal privacy team), investigation related to zero day vulnerabilities (CISA emergency directives), breaches of internal systems, fake website/domains, insider threats, and investigated alerts that turn into incidents.
22	What is the total number of endpoints within the USAC enterprise?	Currently 941 workstations and 1,257 servers/appliances.
23	How many end users within USAC?	The total number of Employees and contractors is currently 2,819.
24	What is the license size and current utilization of the Splunk instance?	USAC is licensed for 500 GB per day and our average for the last 30 days is 350 GB per day.

Q#	Question	Answer
25	What is the license size and current utilization of Carbon Black EDR?	Current license agreement has 1000 windows endpoints and 164 CPU cores. Current usage is 941 on workstations and USAC is currently deploying to servers. We anticipate hitting the server core count when fully deployed.
26	Should the contractor expect to use its own laptops to remotely monitor the USAC environment?	Correct; access to Splunk Cloud and other tools will be provided over SAML using Okta over the internet. Contractor will need to supply endpoints and access for personnel.
27	We did not see a past performance questionnaire attached in the RFP document. In lieu of a questionnaire, is it acceptable to simply list the contact information for our references?	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. This will be completed after proposals are submitted to USAC. Each reference 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.
28	For the past performance references, would USAC consider requiring the prime offeror to submit all references and not use any from proposed subcontractors? By requiring all past performance references come from the prime, we feel this greatly reduces program risk to USAC.	The Offeror can submit past performance references for prime or subprime contracts. There is no requirement that all past performance references originate from the prime contract.
29	Section E: 6.C.3.a / Page 51; After listing the administrative information required in accordance with 6.C.3, there is very little room to provide a convincing narrative of the information required in 3.a. Will USAC increase the page limit for Past Performance Information from 1 page each to 2 pages each?	The page limit will not change.

Q#	Question	Answer
30	Section B: 11.F; Para 11.F specifies Key Personnel as the "Program Manager"; however, Section C: 1.FF specifies "Key Personnel" are "full-time employees of Contractor that are in the positions identified elsewhere in the Contract as those that are required to perform the Services." Will USAC confirm the only "Key Personnel" requirement is for a "Program Manager" and the only resume needing to be submitted is for that specific individual?	USAC does not intend to dictate the size and composition of the ideal team to perform this Contract. The only required position is Project Manager. The Offeror will propose all other Key Personnel and provide their resumes within the submitted proposal.
31	Section B: 10.A; Scope of Services instructs the contractor to create a charter with specific sections. Will USAC elaborate on when the "charter" is to be created and delivered by the contractor?	The charter must be delivered to USAC within five (5) business days of Contract award.
32	Section B: 10.A; Scope of Services instructs the contractor to create a charter with specific sections. Does USAC expect the "charter" to be submitted as part of the solicitation response (Volume II – Technical Capability)?	No, the charter must be delivered to USAC within five (5) business days of Contract award.
33	Section B: 10.A; Scope of Services instructs the contractor to create a charter with specific sections. If required to be submitted as part of Volume II, will USAC increase the page limit from 15 pages to 25 pages to accommodate the additional information?	The charter is not required to be submitted with Offeror's proposal.
34	Section B: 10.B.1; Section 10.B.1 discusses the responsibilities pertaining to security investigations and reporting. Does USAC currently possess any automation capabilities as related to alert detection, analysis, or investigation reporting?	USAC utilizes Splunk Cloud w/ES for automation of detection, analysis, and investigation reporting. ServiceNow is utilized for incident response tracking.
35	Section B: 10.B.4; Section 10.B.4 discusses the requirement for the Contractor to regularly communicate investigations with the USAC IT leadership. Does USAC currently utilize	ServiceNow incident ticketing is used for incident response tracking.

Q#	Question	Answer
	any dashboarding technologies to convey investigation metrics and trend analyses during these communication events?	
36	General; Staffing - Can USAC please provide the number of FTEs currently supporting this effort?	2 FTE incident leads plus 1 SOC manager (Pending).
37	General; Current Contract - Can USAC please provide the current incumbent?	Please see answer to Question 2.
38	Pg 4; Existing FedRAMP Authorized Service Providers have been vetted to meet managed security operations standards. Based on the purpose of the solicitation (24/7/365 managed services and monitoring), and the publicly available approved list of FedRAMP-Authorized Security Operations Center Providers, is USAC amenable to sending data to an externally managed, FedRAMP-authorized, Security Operations Center for additional investigation and response actions? Also, would USAC include FedRAMP authorization as a requirement for this solicitation?	More details required; is this request to ship events out of Splunk Cloud to a separate FedRAMP environment?
39	Pg 5-6; Based on the request for a managed security operations service, can USAC confirm this requirement allows for a 100% virtual team?	Yes
40	Pg 6; Does the COVID policy apply to all resources, including remote/virtual resources?	The COVID-19 Vaccination Validation & Testing Policy applies only to Contractor Personnel that enter USAC premises.
41	Pg 9-10; Alert levels - Is it acceptable to automate responses to Low and Info tickets?	Yes, with sample review to ensure functionality.
42	Pg 10; What is the expected level of effort for daily threat hunting for days that lack meaningful alerts?	2-3 analysts hours per day or as needed based on findings.

Q#	Question	Answer
43	Pg 15; Is the only acceptable certification for Key Personnel a CompTIA CySA+? We recommend acceptance of the following equivalent industry certifications: CISSP, Security+, GCIH	Please see answer to Question 14.
44	Bid Sheet; In order to effectively estimate for this requirement, can USAC provide the daily ingest (GB) expected over the course of this project?	Licensed for 500 GB, current ingestion averages 350 GB/day.
45	Bid Sheet; Given that this is a managed service requirement, would USAC accept pricing bids that are tied to daily ingest volume, as opposed to labor hours?	Only CLIN004 is based on labor hours. CLINs 001-003 are based on a firm-fixed price. All submitted price proposals should follow the directions outlined in the RFP.
46	# 5 Page 7; What is the NTE ceiling price? Refers to Bid sheet but it is not listed there.-#5 page 7	USAC does not provide this information. Offeror should provide its best estimate based on the scope of work stated in the RFP.
47	Page 15- page 16; What are the key positions? Only lists Project Manager. How many key personnel?	USAC does not intend to dictate the size and composition of the ideal team to perform this Contract. The only required position is Project Manager. The Offeror will propose all other Key Personnel and provide their resumes within the submitted proposal.
48	D. Accessibility page 14; In year how many percent of weekends do key personnel need to work? Or is it available by phone?	5%, phone escalation is acceptable.
49	F. Key Personnel page 15; It lists 2-3 full time Contract personnel but does not state position . What are the positions?	Please see answer to Question 47.
50	General Question; It mentions Key personnel and other support positions but we do not list of positions or labor categories.	Please see answer to Question 47.

Q#	Question	Answer
51	-#8 page 23; It refers to labor categories and positions in bid sheet. But not there please request list of labor categories because we need to get the pay rates.	Please see answer to Question 47.
52	General Question; No titles that I can see for Key personnel except for the Project Manager.	Please see answer to Question 47.
53	page 50; Don't have attachment	Attachment A is submitted by the Offeror and includes the resumes of the Key Personnel proposed by the Offeror.
54	General Question; If we are using any partner for SOC and if they are using their dashboard or any agent or tools to gather information for SOC related activities then the tools or the Software's must be Fedramp certified or must have obtained ATO. USAC is currently using Splunk (SIEM), Carbon Black EDR, Proofpoint and Rapid 7 Insight VM for Security event Management and detection which are Fedramp certified.	Not certain on question. Any external connections are required to be FedRAMP Moderate or in process.
55	Is the SOC vendor required to bring on board their tools and subscriptions for Threat hunting and integrate with USAC SIEM? Or does USAC have subscriptions to Threat exchanges (STIX, TAXII, Anomali etc.)	USAC has some subscriptions. Offeror may present recommendations for Threat Hunting and Threat Intelligence for usage within their proposal.
56	What type of threat hunting is expected from the Vendor?	Structured, Unstructured, and Situational hunting.
57	Will the vendor be provided with a sandbox environment to perform threat hunting and perform malware and threat analysis?	USAC does not have a sandbox for these functions.
58	How many endpoints are part of the scope? Is cloud (AWS, Azure, M365) included as well?	Please see answer to Question 22. Cloud endpoints are included in this count. AWS, Azure/M365 are included.
59	Will USAC allow vendor to deploy agents on the endpoints to gather events, logs, alerts to be integrated with Vendor	No; the vendor is expected to use USAC's Splunk Cloud.

Q#	Question	Answer
	managed SOC Dashboard and alerting system or is the vendor required to use USAC monitoring system?	
60	What is approximate number of event and log size generated per day?	Please see answer to Question 19 and 44.
61	What will be the SOC's vulnerability management process?	USAC has a dedicated Vulnerability Management team. SOC will be expected to report risky or potentially exploited vulnerabilities to the USAC Vulnerability Management team.
62	Can USAC provide an estimate of how many incidents are triaged in a week based on severity?	Please see answer to Question 19.
63	What is USAC's Splunk maturity level?	Splunk Cloud.
64	Does USAC require vendor personnel to have Secret Clearance or personnel to be US Citizen, Green Card holders?	All personnel should be authorized to work within the United States. No security clearance is needed.
65	2. What type of threat hunting is expected from the Vendor? 2.1 Hypothesis based hunting based on Analytics, Intelligence driven or Situation Awareness. Does USAC have tools and place to carry out hypothesis based threat hunting? 2.2. Intelligence Driven 2.3 Situational Awareness 2.4 Investigation using Indicator of attack	Please see answer to Question 54.
66	Is it a requirement that the solution be FED RAMP certified?	Yes, any system connecting to USAC must be FedRAMP Moderate.
67	Would USAC consider moving away from SPLUNK and leveraging an alternative SIEM with an SLA backed service component?	No

Q#	Question	Answer
68	Is there an incumbent? Can USAC please provide the details of the incumbent contract?	Please see answer to Question 2.
69	We request USAC to grant an extension of three weeks.	The deadline to submit proposals will not change.
70	General – who is the current incumbent on the USAC SOC contract	Please see answer to Question 2.
71	A.3 Confidentiality 4; Please confirm if the signed Attachment 3 Confidentiality Agreement should be in an appendix at the end of Volume 1 Corporate Experience so that it does not count against the page count. If it is required to be attached in a different Volume please let us know.	The signed Confidentiality Agreement may be submitted as a separate attachment to the Offeror's proposal or included with Volume I. It will not count toward the page limit.
72	B.1. Project Overview 5; 'Contractor shall perform analysis on alerts and logs coming from the USAC IT Systems'. What is the current ticket volume?	Please see answer to Question 14.
73	B.1. Project Overview 5; "team of similar size and scope to the USAC Security Operations team" - What is the size of the existing Security team at USAC?	Please see answer to Question 36.
74	B.1. Project Overview 5; "This includes designating appropriate staffing levels for increased log generation and threat hunting activities." – Is the expectation that the contractor will predict the size of the log generation increases over time?	Potentially, in coordination with USAC personnel.
75	B.3.A. Place of Performance 6; For coverage 24/7/365, how does the expectation that contractors are in the office 2 days a week work? Does that pertain only to 2 days of day shifts or expectations that late night shifts would be in person at USAC? Or are night shifts expected to be in person in a hybrid environment?	SOC analysts can be 100% remote. Splunk support/engineering and Project management may be required to work in office 2 days a week, depending on assignments or technical requirements.

Q#	Question	Answer
76	B.3.A. Place of Performance 6; Please confirm whether the Project Manager Key Personnel needs to be on-site.	Please see answer to Question 75
77	In 3.A it indicates "Presently, USAC has a hybrid work approach requiring contractors that work in USAC's office to be in the USAC office at least 2 days per week'. In 3.E it indicates "While attending USAC Headquarters for meetings or to conduct audits, **Contractor Personnel will be considered as visitors**. **All visitors are required to complete USAC's Visitor Form, and wear a badge while on premises**. Please clarify what roles are expected to be on site 2 days a week. Please clarify that the roles required to be on site 2 days a week will be provided a permanent badge through the life of the contract.	Please see answer to Question 75.
78	B.5. Contract Type 7; Indicates 'price stated in Attachment 1 – Bid Sheet.', however the ceiling is not in the Attachment 1 Bid sheet.	USAC does not provide this information. Offeror should provide its best estimate based on the scope of work stated in the RFP.
79	B.10.B. Overview of Tasks Required 8; Besides the management and administration of Splunk are there any other Security Tools that the Contractor will be responsible for such as EDR. Is it USAC's expectation that the Contractor will be responsible for implementation of new Security tools?	No; Contractor will be primarily responsible for Splunk Cloud management. USAC maintains responsibility for implementation of non-Splunk tools.
80	B.10.B.7 Provide Shared Management and Support for USAC's Splunk Environment 11; Can USAC define the contractor's role in providing Splunk Management, and what additional resources might be provided by another team that is co-managing Splunk.	Tuning alerts, installation and management of Splunk app/TAs, upgrades, automation, and other Splunk Cloud specific tasks as assigned.

Q#	Question	Answer
81	B.10.C. Deliverables and B.11.B Twice Weekly Status Meetings 12 and 14; On page 12, Deliverable # 5 is a Twice Weekly status report. Please clarify if Deliverable # 5 is the same requirement stated in Section 11.B. Twice Weekly Status Meetings? If these are the same deliverables please clarify the second paragraph of 11.B. where it states 'Contractor shall prepare a status report and submit it to USAC once per two weeks whereas Deliverable 5 indicates providing a status report for each of the two meetings during the week.	Two distinct deliverables are expected; Twice weekly report delivered to USAC SOC Manager detailing all activities performed by Contractor, including open vs. closed events, threats detected, incident response hand offs or escalations. Second deliverable is every two weeks to be delivered as an Executive report to Senior Manager of Security Operations, detailing on active and closed incidents, current threats, and security weaknesses discovered. These reports will require maturation as the relationship between USAC and the Contractor is developed.
82	B.11.D. Accessibility 14; 'Key Personnel must be accessible via telephone or email during USAC's normal business hours, Monday through Friday (9:00 AM - 6:00 PM ET) with availability from time to time prior to 9:00 AM and after 6:00 PM and on weekends if project activities and the needs of the business dictate the need for work outside of standard hours.' Our assumption is the PM will need to be present for urgent issues requiring escalation during this time window?	Yes; incident response escalation will require PM or deputy to contact the designated USAC Point of Contact.
83	B.11.F. Key Personnel 15; Do all the members on the team need the certs listed, or just the Key Personnel? Do equivalent certifications or degrees count as replacements, following the "DoD 8570 Baseline Certifications", which provides different tiers for equivalence?	Please see answer to Question 14.
84	B.11.F. Key Personnel 15; Would the Government consider splitting the Key Personnel Project Manager role experience into: 1. A Project Manager with Cyber/CISSP experience and 2. A Cyber Lead SME	Yes, this would be fine.

Q#	Question	Answer
85	C.18.J Additional Requirements for Services in Contractor Owned / Controlled IT: 30; "Contractor shall maintain Contractor Owned/Controlled IT used by Contractor in Performance" is the expectation that the Contractor will provide Computer Systems used by the SOC or will GFE be provided? What is the expectation for the use of Contractor/Controlled IT?	Please see answer to Question 26.
86	C.22. Technology Considerations 35; Do COTS, SaaS, PaaS, or IaaS Software deployed in Contractor Owned and Controlled IT cloud have to be operated in a FEDRAMP environment?	Please see answer to Question 66.
87	C.25. Key Personnel 37; USAC may specify which Contractor employees are Key Personnel under the Contract. – Is this intended to be negotiated or Key Personnel as submitted in response to this RFP?	USAC does not intend to dictate the size and composition of the ideal team to perform this Contract. The only required position is Project Manager. The Offeror will propose all other Key Personnel and provide their resumes within the submitted proposal.
88	E.6. Proposal Content 48; Can a table of contents be added to Volumes 1, 2, and 3 and not count against page count?	A table of contents is optional and will be included in the page limit.
89	Technical Approach: An in-depth discussion of Offeror's technical approach to providing the services outlined in Section B, along with a clear statement of whether or not Offeror's performance of the Contract will comply with all requirements stated in this RFP, and the USAC Terms and Conditions set forth in Section C. **Offerors must submit a detailed response to this RFP. Offeror must clearly state whether it will comply with all requirements stated in this RFP, and the USAC Terms and Conditions set forth in Section C, and provide detailed information about how it will fulfill the requirements of the RFP.**	Technical Capability (Volume II) must provide an in-depth discussion of Offeror's technical approach to providing the SOC 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 the RFP, and the USAC Terms and Conditions set forth in Section C. Any deviations from, or exceptions to, the requirements in this RFP or USAC Terms or Conditions set forth in Section C must be clearly identified in Volume II of the proposal.

Q#	Question	Answer
	Clarification requested. Please note there is some redundancy between the first paragraph (unbolded) and the second paragraph that is bolded.	
90	E.6.B.2 Technical Approach 49; 'Technical Approach: An in-depth discussion of Offeror's technical approach to providing the services outlined in Section B' · Please clarify that for the Volume II, 2.Technical Approach response requirements, contractors should write to 'the services outlined in Section B' starting at subsection 10 Scope of Services and Deliverables (page 8), subsection B. Overview of Tasks Required (page 8), then through the C. Deliverables table ending on page 13). · Going one-step further, please clarify that for 2.Technical Approach response requirement: Contractors should not address Section B: 1. Project Overview, page 5, through 10.A Scope of Services charter bullets on page 8. · Going one-step further, please clarify that for 2.Technical Approach response requirements: Contractors should not address C.11. Meetings, Management sections: A. Project Kick-off (bottom of page 13) through E. Monthly Status Report (MSR) (bottom of page 14). This clarification request helps bound what is required for the Technical Approach section since there are 15 pages that require a detailed approach.	The Technical Capability (Volume II) must provide an in-depth discussion of Offeror's technical approach to providing the services outlined in Section B. USAC is seeking to evaluate proposals that demonstrate the Offeror's expertise in performing engagements of a similar size and scope as illustrated by Offeror's description of how it proposes to perform the requirements set forth in this RFP. USAC does not dictate the approach used to demonstrate how the Offeror will perform the services required for this RFP or the specific sections that should be detailed in the Technical volume.
91	E.6.E.1. Proposal Presentation 51; Please identify what the margin size requirements are for the four sides of the 8.5" x 11" proposal response pages.	USAC does not dictate a margin size requirement. Documents must be readable when printed.

Q#	Question	Answer
92	E.6.E.2 Page Limitation 52; For Volume II Technical it indicates 'may not exceed 15 pages'. Is the Cover page excluded from the 15 page count in this case?	The page limit for this volume includes the cover page and excludes Attachment A – Resumes.
93	Attachment 1 Bid Sheet ; Please clarify what the contractor needs to include in CLIN 4 in terms of estimated hours since the Bid sheet indicates it's optional and TBD.	USAC does not provide this information. Offeror should provide its best estimate based on the scope of work stated in the RFP. CLIN004 is included to allow the Offeror to propose additional services / expertise that may not have been explicitly laid out in the RFP.
94	Attachment 1 Bid Sheet ; Please confirm that CLIN 4 does not fold into the ceiling price.	CLIN004 will be included in the overall NTE ceiling price.
95	P. 3; We understand that the purpose of this RFP is for SOC Managed services - alert/event Triage and Tier 1 support leveraging USAC's Splunk monitoring and SIEM solution. 1. Please clarify if the 24x7 managed services includes Tier-1, Tier-2, and Tier-3 support ? 2. Is it fair to assume that the scope of this RFP is the provide Tier-1 support (including alert Triaging) and escalate to Tier-2 / 3 managed by USAC?	Tier 1 and Tier 2 provided by the Contractor, further escalation is managed by USAC.
96	P. 5; What are specific pain points that USAC is looking to solve through this RFP? - technology gap? Process challenges? Please specify and elaborate	Personnel impact. USAC is looking to solve 24/7 monitoring with limited staff, as well as provide solutions for managing Splunk Cloud.
97	P. 52; How much recent should be our past performance? Does USAC consider past performance within 3 years is considered as acceptable?	Yes, this is acceptable.
98	Is it fair to assume that USAC will own all the tools and licenses required for the SOC operation?	Yes

Q#	Question	Answer
99	We understand that USAC has implemented a Security monitoring system. Please clarify if it is integrated with USAC service management tool like ServiceNow or Eqv?	Yes, USAC Splunk Cloud is integrated with USAC ServiceNow.
100	Please provide volumetric information /current device inventory and respective volumetric of cybersecurity devices and users to be supported as per below: • Number of Firewalls to be supported? • Number of IPS / IDS devices to be supported? • Any other Security appliance /Ruleset Assurance devices to be supported? • Ant-Virus support for end user device - Number of end-user devices to be supported • Anti-Virus support for servers /VM - Number of servers to be supported? • File integrity monitoring (FIM) - Number of servers to be supported? • Managed Encryption- Number of end-user devices to be supported • Host-based intrusion detection systems (HIDS) /HIPS- Number of end-user devices to be supported • Identity and Access Management- Number of end-user devices to be supported	USAC will manage all of these systems. Please see answer to Questions 23-25 for details USAC has provided for this question.
101	P. 9; 7. Provide shared management and support for USAC's Splunk environment " - Please clarify the shared management? Does this means - Tier-1 support by the contractor? and Tier-2/3 by USAC staff?	Please see answer to Question 95 for SOC expectations. Shared management will include details in Question 80.
102	Please clarify if any of the below Threat and Vulnerabilities management activities are USAC retained? 1. Security Patch management 2. Firewall Management	USAC will retain all of these functions with the exception of #7 and #9. These will be shared responsibilities between USAC and the Contractor.

Q#	Question	Answer
	3. Intrusion Detection Prevention System management 4. Penetration Testing 5. Web Proxy Management 6. Security Scanning Tool Management 7. Security Incident and Event Management 8. Threat Mitigation and Remediation Support 9. Digital Forensics Support	
103	Please clarify that the security patch updates and execution of patch management is USAC retained scope?	USAC will retain this.
104	Please clarify that the proactive security activities such as Penetration testing, reactive activities such as "Digital Forensic support" are USAC retained scope?	USAC may requires additional support in an investigation for Forensics as needed.
105	Please clarify activities for 'Threat mitigation and Remediation support" is USAC retained?	The Contractor is expected to provide recommendations for security control findings and incident remediation.
106	We understand that USAC's estimate of 2 to 3 FTEs per shift is sufficient. Could USAC provide clarity for the following: 1. Experience level of the FTEs 2. Which shift hour requires maximum support and hence higher FTE count? 3. Any of the existing staff to be hired as part of the contract?	1. At least one Tier 2 for escalations 2. Business hours (9am-5pm) is primary, Second shift (5pm-1am) is secondary 3. There is not a current incumbent contract for these services.
107	Please provide details of the IT automation implemented. What automation tools are currently in use in the USAC environment?	SOAR implementation within the next 12 months. Event alerting and ticket creation is currently implemented between Splunk Cloud and ServiceNow.
108	Please share the ticket details (Incidents and Service requests) of last 6/12 months of the SOC operation and Tier-1 support. This will help us to better understand the environment.	Please see answer to Question 19.

Q#	Question	Answer
109	Page 1, Project Overview How much daily ingest based upon the tools, applications, and infrastructure that is currently in-place does USAC see on a daily basis?	Please see answer to Question 24.
110	Page 6, Place of Performance USAC notes that the "Washington, D.C. 20005 (“USAC Headquarters”), virtually, or such other location as USAC may approve in its sole discretion. Presently, USAC has a hybrid work approach requiring contractors that work in USAC’s office to be in the USAC office at least 2 days per week." Can you please confirm, if agreed upon and approved by USAC, that resources that are virtual in nature would be excluded from the hybrid work approach?	Please see answer to Question 75.
111	Page 8, Task B, Bullet Point 7, Overview of Tasks Required How many notable events per day does USAC current receive on average?	Please see answer to Question 19.
112	Page 8, Task B, Bullet Point 7, Overview of Tasks Required Are all event flowing into Splunk Common Information Model (CIM) compliant?	~90%. Some maturity is needed, but CIM/data model compliance is expected.
113	Page 9, Bullet 1, Conduct Security Investigations USAC notes that the "Contractor will use security tools that USAC’s Security Operations team have implemented in the environment. These well-known security tools are prevalent in the industry and are listed in Attachment 2." Can USAC confirm that active tuning and engineering support has already / will be available in order to continue to tune alerting on each security product?	USAC support teams will provide engineering support for these products. Splunk tuning is part of this contract.

Q#	Question	Answer
114	Page 11, Bullet 7, Provide Shared Management and Support for USAC's Splunk Environment Has tuning for current notable events already been undertaken and is a process established at present for future tuning request? While it is stated that the Managed Service provider will undertake and tune security alerting, data input creation, etc. will they become the primary interface for these engineering items or will it remain a collaborative exercise with other USAC engineering teams?	This will remain a collaborative exercise between USAC and the Contractor. USAC Security engineering will be available for this function.
115	Page 15, Are there other certifications comparable to the CompTIA CYSA+ also considered adequate to meet key personnel requirements?	Please see answer to Question 14.
116	Section 18 C. states, "In the event a direct interconnection is to be established between Contractor Owned / Controlled IT and USAC IT Systems, the Data Security Liaisons shall execute an interconnection security agreement prior to the establishment of such direct interconnection." Will USAC provide IT systems and software necessary for the performance of this contract or should the Contractor include these resources in the bid price?	Please see answer to Question 26.
117	Does USAC required contractor owned/controlled IT systems interconnected with USAC IT Systems to meet Trade Agreements Act requirements?	Not sure on the nature of this question. Please provide more clarification: is this referring to Trade Agreements Act (TAA)? If so, the TAA does not apply to USAC. See Section C of the RFP for all Terms and Conditions specifically Section C. 42. NATIONAL SECURITY SUPPLY CHAIN REQUIREMENTS
118	Concerning the need for daily threat hunting activities, does daily reference calendar or business days?	Business days.

Q#	Question	Answer
119	SOW pg. 5; a. If USAC does not have a contract with FCC, how is this program funded? b. Does USAC receive any funds from FCC or any other government entity?	As an independent not-for-profit designated by the FCC, USAC administers the Universal Service Fund (USF). The Universal Service Fund is paid for by contributions from providers of telecommunications based of an assessment on their interstate and internation end-user revenues.
120	SOW pg. 6; Will USAC provide a copy of the USAC's COVID-19 Vaccination Validation & Testing Policy?	USAC follows the policies outlined by the CDC. https://www.cdc.gov/coronavirus/2019-ncov/
121	SOW pg. 21; 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: Accept the Services and Deliverables; or Reject the Services and Deliverables and advise Contractor of the reasons for the rejection." This statement does not show how long USAC has to accept services and deliverables. How will USAC accept the services provided? Will USAC provide a detailed timeline for the delivery of deliverables?	USAC uses the Deliverable Acceptance Form attached to the RFP to accept services provided. USAC does not provide a detailed timeline for the deliverables. Please refer to the deliverable table in Section B.10.C. for the expected timeframe for each deliverable.
122	SOW pg. 24; Does USAC foresee this program not making it to 3 years?	The initial term of the awarded Contract shall be for twelve (12) months, with two additional one (1) year option terms to be exercised by USAC in its sole discretion.

Q#	Question	Answer
123	Is this work currently being provided for USAC? If Yes, Who is currently providing this service for USAC? How many FTEs are currently providing this service?	No, this is currently done by USAC personnel. Please see answer to Question 36.
124	How many events are currently being monitored?	Please see answer to Question 19.
125	How many incidents required a response in the last 12 months?	Please see answer to Question 19.
126	Does the scope of the RFP include the Splunk Platform Management tool?	Yes; Contractor and USAC will have a shared responsibility in maturing the Splunk Cloud platform.
127	Request USAC to provide the details of the current Splunk deployment architecture. i. HA and DR In place for the whole Splunk platform (apart from HA and DR offered at the application layer), ii. Single-site or multi-site indexer cluster iii. Any search head cluster in place iv. Instances of indexers, search heads, and other management components (deployment servers, cluster master, search head deployer, licence master, DMC, etc.) v. Log forwarding (data collection) architecture/data sources (UFs, HFs, HTTP Event Collector, KAFKA, Syslog, etc.) vi. Indexer Storage (any object storage such as Smart Store or S3 in place)?	Please see answer to Question 3.
128	What is the average daily licence utilization?	Please see answer to Question 24.
129	Any premium threat intelligence tools (if any) integrated with the existing Splunk platform?	Splunk Enterprise Security with custom OTX. No other premium threat intel integrated.
130	Splunk Enterprise Security (ES) requires data to be compliant with the Common Information Model (CIM) for	Please see answer to Question 112.

Q#	Question	Answer
	normalisation. While we understand Splunk ES is already built, can USAC confirm if the existing data sources onboarded in the Splunk Core platform are CIM compliant?	
131	Is Splunk already integrated with the ticketing system (ServiceNow) for incident workflow?	Partially, some maturation is required for full automation.
132	What is the estimated increase in ingestion and devices per quarter?	Estimates are +10% ingestion per year.
133	Can you provide the procedures in place for the backup and restoration of the various Splunk components?	Please see answer to Question 3. USAC Splunk is operated in Splunk Cloud GovCloud; backup is handled by Splunk.
134	How is the Splunk platform availability monitored?	Please see answer to Question 3. USAC Splunk is operated in Splunk Cloud GovCloud; availability is handled by Splunk.
135	Please share the policies in place for scaling up of the Splunk environment (e.g. A new input resulting in huge data ingestion resulting in high disc space and licence usage)	Please see answer to Question 3. USAC Splunk is operated in Splunk Cloud GovCloud; expansion is handled by Splunk.
136	What is the proposed method for our SOC analysts to connect into the USAC environment (Splunk, SOAR, ITSM, etc.)?	Please see answer to Question 26.
137	Can USAC provide us with the average monthly alert count that is generated in Splunk and an approximate percentage of these alerts that are qualified as true positive security incidents?	Please see answer to Question 19.
138	Does USAC have an existing service provider managing the current SOC operations using Splunk? If yes, would any of the content (apps, technology add-ons) developed by the current provider be retained in the Splunk platform?	Please see answer to Question 2.

Q#	Question	Answer
139	Are there any specific reports that the SOC team is required to generate on a daily, weekly, or monthly basis to meet any internal and/or external compliance needs?	Please see answer to Question 81.