Universal Service Administrative Company (USAC)
USAC IT Security Operations Center – IT-22-159
Questions & Answers

Q#	Question	Answer
1	Is there any incumbent contractor working on this project? If yes, can the government please provide the incumbent details including contract value and period of performance?	There is not a current incumbent contract for these services. Normally, USAC does not provide information regarding incumbent contractors. USAC is not a federal government agency.
2	Can the government please provide historic data of estimated tickets for SOC support?	Provided will be on average for the last week. Over the last week Critical: <5 per week High: <10 per week Medium: <100 per week Low: <2,500 per week
3	How many incidents does the government anticipate every month?	Based off USAC's history, we anticipate two defined security incidents per month.
4	Can the government 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.
5	Can the government please provide historic or estimated Level of effort?	Incidents can take from a few days to a few weeks depending on the amount of investigation needed.
6	Can the government provide more details on how the tickets are assigned?	Tickets are selected and created by internal Security Analyst. Workflows can be changed within ServiceNow to assign tickets at any time based off the request of the selected vendor.

7	If this is a follow-on contract, please provide insight into the incumbent contract - including Incumbent Contractor name, Contract Number & Period of Performance?	USAC does not provide information regarding incumbent contractors.
8	Please share the estimated level of effort.	Based on the Scope of Work and Deliverables, Offerors should estimate the required level of effort.
9	Is this new work or a follow-on contract for existing work?	This is a new requirement. See answer for question 1.
10	What is the total number of endpoints within the USAC enterprise?	Currently 941 workstations and 1,257 servers/appliances.
11	How many end users within USAC?	The total number of Employees and contractors is currently 2,819.
12	What is the license size and current utilization of the Splunk instance?	We are licensed for 500 GB per day and our average for the last 30 days is 424 GB per day.
13	Is Splunk deployed on-prem or in cloud?	Splunk is deployed in the FedRAMP Cloud.
14	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 we are currently deploying to servers. We anticipate hitting the server core count when fully deployed.
15	On average, how many documented event investigations occur per month?	84 events investigations are processed per month on average. This is a low number due to current resources. More are expected to be processed.
16	On average, how many confirmed incidents are processed per month?	On average we experience two confirmed incident per month.
17	On average, how many threat hunting cases are reported daily?	Currently USAC is not conducting threat hunting exercises.

18	Do the RFP awardee's personnel supporting this effort need to reside within the geographical area (e.g., less than 100 miles of the Washington DC area) in case of a cybersecurity-related outage?	USAC would like to have a Project Manager available to onsite on a regular basis for check-ins. The team itself can be remote and is not required to come into the office.
19	Does section D. include government furnished computers for dedicated SOC operations?	USAC does not provide government furnished computers as we are not a government organization. Access will be granted to Cloud-based tools, SOC is expected to be able to provide their own workstations.
20	Does section D include separate dedicated SOC workspace only for SOC operations?	There is not a separate dedicated SOC workspace within USAC for SOC operations. A dedicated set of cubicles and managers can be provided.
21	Does section G. focus on "business continuity plans, disaster recovery plans, emergency operations plan and procedures, and associated plans and procedures" only for work under IT Security Operations Center (SOC) Services for the RFP?	This section applies to the section of the vendor that is selected that will be providing SOC services to USAC. This clause is intended to ensure we have coverage in the event a vendor is displaced.
22	Please confirm this requirement - may bidders be considered if they do not have a record or embedding resources into existing USAC Security Operations Team? If so, does that imply that only incumbent contractors may bid?	There is not a current incumbent contract for these services. Bidders will be required to use their resources to work with existing resources at USAC to form a cohesive SOC.
23	Is the ServiceNow ticketing system accessible by all USAC personnel and contractors?	ServiceNow is available to all contractors and staff. Currently it is used just by security personal.
24	If ServiceNow is also used by the awardee of the RFP contract - specifically for cybersecurity-related investigations (especially those investigations that involve USAC users' accounts and their activities), what measures are enabled in ServiceNow to isolate/restrict access to and protect cybersecurity investigations from potential compromise?	ServiceNow is primarily used by the Security Operations team and security controls have been implemented to assigned tickets to specific groups with the ITSM module. Additional security parameters can be configured if needed.
25	If ServiceNow is not used for cybersecurity investigations, what alternate ticketing system do you use for investigations that involve USAC users' accounts and their activities?	ServiceNow is used for tracking all security investigations.

26	If neither ServiceNow nor an alternate ticketing system is being used for investigations that involve USAC users' accounts and their activities, would the USAC Security Operations Team open to using a self-contained cybersecurity ticketing system (e.g., We developed and implemented CDCTracker for OCC CDC for that purpose).	USAC is using ServiceNow for its investigations and incident response tracking tool.
27	Regarding monitor the environment, how many endpoints, servers, network devices are in the environment? Does "environment" cover production, development, DMZ?	Production and non-production devices in our DMZ is about 100.
28	Is auditing compliance referring to ISSO duties (auditing of systems as it relates to NIST 800-53 Rev 5), or auditing the contractor's performance on the contract?	The vendor that is selected for this contract will be expected to provide artifacts to support annual FISMA audits and ATO/Continuous Monitoring assessments, such as proof of incident response, investigations, and other supporting documents when requested.
29	Does 24x7 cybersecurity support in support of Security Operations Center (“SOC”) services refer ONLY to the Cybersecurity Event Monitoring (CEM) team, or does USAC Security Operations expect 24x7 coverage by all RFP contracted cybersecurity teams (Incident Response, Security Engineering, Vulnerability Management, Threat Intelligence, and Identity/Access Management)?	USAC expects the selected vendor to provide Cybersecurity Event Monitoring (incident response and threat intelligence).
30	For Phishing exercises, what tool(s) does USAC Security Operations use (e.g., Cofense)?	Proofpoint Security Awareness Training (PSAT).
31	Knowledge based articles to be stored in what application, format? What is current table of content of KB articles and KB active number of KB articles?	We currently use ServiceNow for our knowledge base and have 13 articles currently. We are continuing to build this out.
32	TableTop audience is cybersecurity only or IT wide or enterprise wide?	Table top exercises will be enterprise wide.
33	USAC would define "initial triage" as determination that cyber event should be escalated as incident using "incident	Correct.

	response plan and procedure to outline reactive actions that need to be taken when reporting, triaging, and mitigating threats or other activities."?	
34	Audit and Compliance Support per NIST 800-53 Rev.?	NIST 800-53 Rev 5
35	Which group manages criteria for Critical, High, Medium, Low and Info categorization of alerts and users concerns?	Our Security Engineering team uses Splunk Enterprise Security that will provide these classifications. This group will also be in charge of fine tuning the alerts for the criteria.
36	Per section B7, how many alerts and user reported concerns in total were investigated in the past Fiscal Year? What were the highest monthly total and what were the lowest monthly total of alerts and user reported concerns in the past Fiscal Year? What was the highest number of alerts and user reported concerns rated Critical, High, Medium, Low and Info in a one month period?	In the past year, we have entered in 394 tickets for security investigations that were manually entered by our security analysis. It is not documented in the ticket the criticality of the alert in an easy way to obtain a report. Sep-21 28 Oct-21 33 Nov-21 16 Dec-21 11 Jan-22 26 Feb-22 18 Mar-22 29 Apr-22 28 May-22 41 Jun-22 59 Jul-22 56 Aug-22 49
37	How many alerts are seen on average per week broken out by the Critical, High, Medium, and Low categories?	Over the last week Critical: 0

		High: 0 Medium: 56 Low: 1,951
38	Is there an existing content engineering/alert tuning process the SOC would feed into?	Members of the SOC team can submit tickets to the in house security engineering team and request tuning.
39	Please confirm if subcontractor recent experience references are allowed.	Subcontractor experience will be accepted.
40	Can USAC please provide Attachment 1 – Bid Sheet in an Excel spreadsheet?	Yes, the Bid Sheet is attached with the Q&A.
41	Are there any SaaS or third-party services for consideration in scope?	No.
42	Is "synthetic transaction output" of security controls required as artifacts for audits?	USAC is not sure what this question means.
43	Will the contractor be responsible for validating the "remediation action" and collecting artifacts to be included prior to closing tickets?	Vendor will be required to work with our POA&M team to document the required remediation and close out investigation ticket.
44	Is USAC requesting full tool management in addition to addressing the alerts of these tools (Splunk Enterprise Security, Carbon Black EDR, Proofpoint, and Rapid7 Insight VM)?	USAC has an internal team of Security Engineers that manage, maintain, and configure all security tools.
45	Is the scope of the monitoring and remediation inclusive of failover sites?	Yes.
46	Please confirm that the Key Personnel can possess higher level qualifications than CYSA+ if he/she does not possess that specific qualification?	Key Personnel can have a higher level of qualifications if CYSA+ is not possessed.
47	How many hosts (server and workstation) are to be monitored/in-scope?	Currently 941 workstations and 1,257 servers/appliances.
48	There are talks in the SOW of ServiceNow as the ticketing system that the USAC uses to track incidents. Does the	Not currently.

	USAC also use the SecOps and GRC modules of ServiceNow?	
49	Would the Splunk Enterprise Certified Admin or Splunk Certified Power User certifications suffice for the Splunk Fundamentals training requirement for Key Personnel?	Yes.
50	Is the USAC leveraging Splunk Cloud? Or an on-premise deployment?	Splunk Cloud.
51	Are all the tools mentioned in Attachment 2 of the PWS sending data/integrated with Splunk?	The majority, yes.
52	For real-time internal collaboration and alerts, does USAC use a tool such as Microsoft Teams or Slack?	USAC uses Cisco WebEx Teams for real-time collaboration.
53	Is the USAC following any compliance frameworks at the host level such as CIS Benchmarks or DISA STIGS?	USAC utilizes CIS Benchmarks.
54	Does the USAC want the selected contractor to provide dedicated Security Operations Center analysts? Or can the Technical Project Manager be dedicated and the analysts provide support to multiple customers if the company offers SOCaaS? Or is this up to the vendor to decide what will meet the requirement/goals best?	USAC does not require dedicated SOC analysts, only a dedicated project manager and/or lead analyst to act as liaison and primary point of contact. This is up to the vendor to determine the best method and approach that meets the requirements and goals of the contract.
55	Will USAC please clarify if Volumes 1, 2, and 3 may be submitted in either Word or .pdf format as acceptable "Electronic" means?	USAC prefers proposals be submitted in PDF format, but will accept proposals in Word format.
56	Will USAC please clarify what the 3-page limit of Volume 4 - Price is for (since it's an Excel workbook)? Is it for a supporting narrative?	Volume 4 of the proposal should be submitted as a PDF and include the cover sheet as specified in the RFP. Volume 4 can include any additional details the Offerer wishes to provide to support their pricing up to the 3 page limit. The Bid Sheet may also be submitted in Excel format as an additional attachment.
57	Will USAC please clarify where the completed and signed page 1 of the RFP is being included with the Offeror's proposal submission (e.g. as a separate attachment)?	The cover page should be signed and returned with the proposal response. Please submit this page with Volume 1 – Corporate Information.

58	Can you please let us know if this is a new requirement? If not, may we receive the incumbent's contract number?	Please refer to Question #1.