Universal Service Administrative Co. (USAC)
IT-24-160 Vulnerability Disclosure Platform
Questions & Answers

Q#	Question	Answer
1	Does USAC intend to have one collective VDP that includes all programs or is there a need to separate each program individually. I.e. separate embedded submission forms on USAC's website for each one and separate listings for each program on Bugcrowd's side. Or can there be one embedded submission form on USACs website and within Bugcrowd's platform that captures all programs?	A single/collective VDP should be fine for USAC's needs
2	Regarding FEDRAMP requirements, will this be a hard set requirement? There is only one vendor currently in this space that is FEDRAMP certified.	FedRAMP requirement is desired, but USAC must first identify that the service satisfies our needs.
3	If FEDRAMP is not a hard set requirement, can you provide what alternative ATO compliances, security controls, and/or documentation would be most preferred by USAC from a vendor?	If FedRAMP certification is not part of the offering, the requirement would be for a suitable substitute certification such as ISO 27001 or SOC 2 Type II.
4	Regarding Section 5. Scope of work and Deliverables Section B Reporting "Within 24 hours, the Contractor will provide validation of fully triaged report to USAC." Can USAC clarify within 24hrs of what event? Submission, First Touch? Does USAC expect all levels of vulnerabilities to be validated, triaged and reported back to USAC within 24hrs, or just higher criticality ones? Our standard SLO is that all P1s are to be touched within 1 business day. P2-P5 within 3 business days. We have additional plan packages that could accelerate those times. Can USAC clarify what is expected on Triage and Validation timeframes based on the specific criticality of the finding.	The SLA is primarily for vulnerabilities identified by submitter at a higher criticality and with which the service triage agrees.

Q#	Question	Answer
5	Regarding Section F. System Architecture/Security and Operational requirements: Address the hosting provider's SLAs and if USAC has the option to negotiate them. Bugcrowd is hosted in AWS and therefore follows all of their standard SLAs and are unable to deviate from them/USAC would not be able to negotiate them. Please confirm if this is acceptable	A level of SLA as aligned with AWS, or an IaaS Cloud Vendor is likely to be acceptable.
6	Could you please confirm the total number of endpoints that will be in scope for the vulnerability monitoring as outlined in the RFP? This information will help us ensure an accurate and comprehensive proposal submission	Approximately 100 externally exposed IP addresses.
7	We would like to inquire about the page number requirements. If we include a table of contents in each volume, will the table be counted towards our total page count or not?	Since USAC does not requires table of contents, that will be counted toward the page limitation.