Universal Service Administrative Co. (USAC)
RFI IT-24-169 – Supply Chain Risk Management Tool
Questions & Answers

Q#	Question	Answer
1	Is there a projected number of companies/suppliers for assessment and monitoring to be used in the pricing model?	Please see a detailed response at Q42
2	Does USAC intend to run this SCRM tool in the cloud? If so, do they have a preferred cloud provider?	USAC will be able to make a decision relative to premise COTS, deployment of COTS in AWS, or a Software-as-a-Service (SaaS) cloud-based solution. All three of these types of tools are used by USAC.
3	Is FedRAMP a requirement? Are there other technical requirements that must be met by the vendor beyond "FISMA and NIST requirements as applicable to federal agencies"?	We are required to seek a FedRAMP solution, however, if not FedRAMP certified, then we would look for FISMA compliance or alternative security compliance / confirmation for the service or product.
4	Is there a planned/ideal go-live date? How much pressure is there to get a solution in place?	The ask is for information not a proposal. Please advise if a product has some defined timelines to implement or planned emergent significant versions in 2025.
5	Do you intend to integrate vendor/supplier information from any exchange type data sets?	If you are able to provide this capability, we would be interested in learning about it.
6	Are you able to provide more information about the quantity and type of vendors/suppliers that will be assessed and the frequency of the assessments?	Developers and suppliers of IT software (COTS or cloud-based), IT hardware (primarily laptops, workstations, and server blades)
7	Can you define "timely" with respect to alerts when a vendor in USAC's supply chain is impacted by a cybersecurity incident?	For incidents, we would expect timeliness to align to closely follow initial public notices, news items, or CVS notice from CISA.
8	Our solution provides an Open API, and we have extensive experience integrating with a number of "procurement applications". Is there a particular "procurement application" in mind?	We have a current procurement tool, but we need flexibility to choose a different procurement tool as needed.
9	Are you able to approximate the number of user and admin licenses required?	5 to 10 user licenses. Admin licenses is dependent upon the tool configuration.
10	In order to provide a more accurate estimate for integration and overall project management services to lead the implementation effort, are you able to	Platform integration is with a procurement/purchasing tool (COTS). See response to #42

	provide more information on the number and complexity of your current processes, workflows, and requirements? What is the integrated platform referenced? How many users will require training?	
11	Would you consider holding an industry day or otherwise arrange for conversations or demonstrations with potential vendors? This would enable the vendor pool to further refine technical approaches and pricing in response to your requirements.	No demo would be required related to the RFI
12	Regarding functional capability outlined under technical requirements in section 4, can you clarify what "sub-tier information" and "communication technology (ICT) supply chain" mean here in context? Is the request here to provide/store security standards compliance, SOC reports, etc. on the direct vendors or the identified sub-tier vendors (or both)?	NIST defines "Information and Communication Technology (ICT)" to include "all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks)." USAC desires the capability to discern to the extent possible a vendor's visibility into its own supply chain. Vendors with low visibility into where their code, components, and other inputs come from are inherently higher risk. USAC would send a customized questionnaire to discern this. Security standard compliance and SOC reports, etc. would apply to the vendor itself.
13	Regarding functional capability outlined under technical requirements in section 5, what additional types of information are expected for a vendor risk profile? Which risk domains should be prioritized aside from cybersecurity, if any?	The purpose of the tool will be to help USAC evaluate potential vendors' cybersecurity.
14	Regarding functional capability outlined under technical requirements in section 6: a) What formats are the SBOMs expected to be obtained from vendors? CycloneDX? SPDX? Both? b) What about the formats for HBOMs?	There's no current format preference. If the SCRM tool had this capability, it would be an added bonus as USAC would potentially be interested in integrating such a function into its evaluations in the future. Yes, using BOMs to spot check for known vulnerabilities prior to purchase or renewal would be a potential use case.

	c) How does USAC plan on ingesting and analyzing the SBOMs and HBOMs data for vulnerabilities? d) Does USAC plan to use CISA's Vulnerability Exploitability eXchange (VEX) documents from vendors to communicate the exploitability of vulnerabilities?	
15	Regarding functional capability which requires a sample workflow of investigating supple chain risk, would it be sufficient for this to be visualized with screenshots / pictures of the actual tool? What is the expected format of the response in its entirety (text-only or okay to include visuals)?	USAC has no preference.
16	Would USAC please clarify whether this is a new requirement or an existing contract? If it is an existing contract, please provide the relevant details, including the contract number and period of performance.	New
17	If USAC determines that a demo is required based on the RFI submissions, could USAC please provide an estimated timeframe for when offerors should plan to conduct the demo?	No demo would be required related to the RFI.
18	If the procurement advances to a Request for Proposal (RFP) phase, could USAC please provide an estimated timeline for the RFP phase? At a minimum, could USAC provide the estimated RFP release date and the expected/estimated RFP response due date.	USAC cannot provide this information at this time.
19	Please clarify if the term "vendors" - as used throughout the Technical Requirements section, are "vendors" the entities supporting USAC's operations or the service providers involved in supporting the Universal Service Fund (USF) programs? Alternatively, does it apply to both?	Software, hardware, and IT service providers, resellers, manufacturers, affiliates and subsidiaries.
20	Please provide background information on the anticipated number of vendors that would fall within the scope at the start of the potential contract? Additionally, is there an expectation that the number or complexity of	See answer to #42. Number/complexity of vendors will remain similar, given that change in market or risk landscape is unpredictable.

	vendors will increase or decrease over the duration of the contract?	
21	Please provide an estimated number of vendor deep dives that will be required per contract year to build vendor risk profiles? This information will help us accurately estimate pricing related to the requirement: "Assist in vendor deep dives from open source information to help build out a vendor risk profile."	Less than 100/year
22	Please provide additional details regarding the expected API integration capabilities for the proposed solution? Specifically, please provide background on the number and general information regarding existing systems or procurement applications that the API must integrate with, and what are the key functionalities or data exchanges anticipated in these integrations?	Example use cases: 1- An asset manager creating a purchase request would be able to check if any supply risks have already been identified for the product or supplier. A product that is deemed to be a covered article (introduces supply chain risk due to role/function of the software, service, or hardware) generates communications and supports assessment of supply chain risk based on responses from the vendor.
23	Would USAC allow for one (1) additional page to be included in the RFI submission to provide procurement and technical recommendations to be considered during the RFI stage?	USAC would not need any additional information at this time. If and when USAC initiates an RFP, we would be interested in such information.
24	How many vendors and/or potential vendors could be assessed through this C-SCRM program (What is the known vendor/supplier population)?	Please see a detailed response at Q42
25	How many supplier questionnaire assessments are anticipated monthly or annually? How many deep dives are anticipated monthly or annually?	Please see a detailed response at Q42
26	Are there specific triggers or events that would prompt an ad hoc evaluation?	We are looking for the supply chain tool to let us know the kind of events that would prompt reexamination of a risk assessment. For example, acquisition or merger of a vendor, or significant/public security failures.
27	Is there a requirement for external vendors to interact with the tool (e.g., provide data, respond to questionnaires)?	Today we send data calls to vendors when we need to assess their supply chain risk, but

		that is manually managed. Automation would be helpful.
28	The requirements reference a request to integrate with an API. Are there specific external data sources the SCRM tool will need to connect to, such as the FCC exclusion list that could be leveraged as an input to complete supplier risk assessments or is this API requirement only related to existing procurement software the SCRM tool will need to integrate with?	This is related to the need to automate the supply chain checks with the procurement system to the extent possible/reasonable.
29	Does USAC have any specific supplier risk criteria that needs to be assessed or will the standard SCRM risk criteria suffice?	Standard for the Federal guidance on supply chain risk management.
30	Should the C-SCRM process and tool align to NIST 800-161, NIST 800-53 rev5 and other regulations (i.e., Executive Order 14017)?	This would be very helpful, especially NIST 800-53 Rev 5 and 161r1.
31	Is USAC seeking a managed service to support supplier assessments (e.g. contractor resources to conduct assessments) and development of all associated C-SCRM processes post tool implementation?	No.
32	Should the pricing estimate be based on one year or a multi-year estimate that would include C-SCRM program build and operate? If a multi-year estimate, how many years (in total) should the factored into the price estimate?	1 year estimate will suffice. No problem if also providing impact of multi-year discounts.
33	Will USAC consider directly purchasing licenses if a vendor proposes a COTS SCRM tool that they would deploy and implement in USAC's IT environment as opposed to a vendor reselling licenses?	Yes.
34	Are there any incumbents performing this work? If so would USAC be willing to disclose the incumbent firms?	There is currently no incumbent.
35	Will this be a Multiple Award Contract?	This RFI is not a solicitation and will not result in an award or contract.
36	Will this contract use a specific contract vehicle (SEWP-VI, Alliant, OASIS, etc.)?	No. USAC is not a Federal entity and will not use any Federal contract vehicles.
37	Does USAC anticipate this will be Full and Open Market Competition or Small Business Set-Aside?	This RFI is not a solicitation and will not result in an award or contract
38	Could information be provided as to the kind of end user which will be leveraging this tool (acquisition user, supply chain user, etc.)?	Primary users will be procurement, asset management, and IT Security for supply

	Will all end users serve the same function and be leveraging the tool for the same goal or will there be a mixture of end users with different functions and goals?	chain risk. Secondary users will be OGC and IT Architecture/
39	Regarding “Availability such that it can be used to evaluate vendors prior to purchase/license renewals as well as on an ad hoc basis after purchase/renewal.” Could further information be provided as to what kind of evaluations USAC is seeking to perform (stability, financial risk, etc.)?	USAC performs evaluations of the cyber security and compliance risks associated with the inclusion of a potential vendor, product, or service in USAC’s ICT supply chain. While stability, financial risk, and other factors may be included in risk assessments, the RFI is specific to evaluation of vendors’ cyber security postures and practices.
40	Regarding “Ideally, the tool would also be able to obtain useable software bills of materials (SBOMs) and hardware bills of materials (HBOMs) from vendors.” Could further clarification be provided as to what specific information be being sought for SBOMs and HBOMs?	A tool capable of obtaining SBOMs and/or HBOMs would be attractive to USAC from a future capabilities standpoint. The ability to catalogue and trace the origins of code, components, and other inputs would potentially be helpful in evaluating the risk associated with a particular product.
41	Is the first page of the RFI which includes the fillable sections “CONTACT INFORMATION” and “OFFEROR SIGNATURE” a required component of a compliant RFI response?	Yes, USAC requires the first page to be completed and returned with each response.
42	How large is the universe of entities USAC anticipates investigating annually? Can a breakout be provided for United States/Canada vs. International entities? This information will be helpful in providing the requested Pricing Estimate.	- Less than 300 per year Most entities will be US; however we are interested in all international partners, affiliates, and influence on the product supplier, integrator, manufacturer, and reseller.
43	Are there any incumbents performing this work? If so would USAC be willing to disclose the incumbent firms?	There is currently no incumbent
44	Regarding requirement 7 - are there particular integrations that USAC would like to leverage?	Integrations with USAC’s procurement system.
45	Does USAC require MFA for the platform?	Yes, USAC uses Okta.
46	Would USAC prefer that data be updated daily with the results of scans hitting an organization’s vendor attack surface for vulnerabilities and weaknesses?	We have not determined a timeframe for refresh of knowledge about vendor products.
47	How many suppliers/companies will need to be monitored?	Please see a detailed response at Q42