Fact Sheet & RFI

Background

GSA, Information Technology Category (ITC) is releasing a Request for Information (RFI) to the vendor community to obtain feedback regarding the developed Cybersecurity Supply Chain Risk Management (C-SCRM) assurance questionnaire and readiness for Post Quantum Cryptography. The developed questionnaire would enable the GSA, ITC to coordinate the collection of relevant Cyber Supply Chain Risk Information (C-SCRI) to improve customer agencies' ability to effectively assess and evaluate the cybersecurity supply chain assurance related to ICT products and service offerings in the GSA federal IT marketplace.

GSA, ITC created the revised questionnaire by leveraging the Cybersecurity and Infrastructure Security Agency's (CISA) ICT Task Force - *Vendor Supply Chain Risk Management Template*. This template was developed in a collaborative effort between the public and private sectors, under the ICT Task Force Workgroup Four (WG4) chartered effort. It specifically incorporated other government standards and industry's best practices from NIST SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC v2.0), and Outsourcing Network Services Assessment Tool (ONSAT).

GSA is aware of the Office of the National Cyber Director's (ONCD) request for information (RFI) on the harmonization of cybersecurity regulations and is actively working closely with ONCD and will inform on next steps based on feedback from the RFI. We recognize the importance of this initiative in addressing regulatory challenges and enhancing cybersecurity across critical infrastructure sectors.

The questionnaire consists of 158 questions, divided into 91 main and 67 follow-on questions and is fundamentally consistent with NIST 800-53B assessment baselines. Depending on the vendor's offerings (product, service, or both), they will encounter different subsets: 158 for products, 126 for services, and 158 for combined offerings. It covers eight different focus areas: general questions, supply chain management and governance, secure design and engineering, information security, physical security, personnel security, supply chain integrity, and supply chain resilience.

To streamline the process and reduce the burden, vendors would only need to submit the relevant questionnaire once based on their offering type. They will receive annual reminders for voluntary updates. This completed questionnaire can also be utilized for other contract responses.

SECTIONS	OFFER/PROVIDER TYPE A	OFFER/PROVIDER TYPE B	OFFER/PROVIDER TYPE C
	Product	Service	Product & Service
GENERAL QUESTIONS	7	7	7
SUPPLY CHAIN MANAGEMENT AND SUPPLIER GOVERNANCE	18	13	18
SECURE DESIGN AND ENGINEERING	7	1	7
CYBERSECURITY	51	51	51
PHYSICAL SECURITY	21	13	21
PERSONNEL SECURITY	29	29	29
SUPPLY CHAIN INTEGRITY	17	4	17
SUPPLY CHAIN RESILIENCE	8	8	8
TOTAL	**158**	**126**	**158**

A viewable copy of the questionnaire is located here.

MRAS RFI Questions:

1 Federal agencies are expected to follow the guidance in NIST SP 800-161 r.1 to implement supply chain security practices when purchasing ICT products and services. The NIST guidance provides the relevant control domains and templates for gathering supplier C-SCRI. For example, NIST SP 800-161 r.1 section 4.1 includes guidance on, 1) Information Gathering and Scoping Analysis, 2) Threat Analysis, 3) Vulnerability Analysis, 4) Impact Analysis, and 5) Risk Response Analysis. The C-SCRI information gathered will enable agencies to evaluate and characterize the level of threat to the integrity, trustworthiness, and authenticity of the product, service, or supplier.

Based upon initial review, do you think the focus areas and responses to the GSA, ITC C-SCRM questionnaire will be adequate to address Cybersecurity Supply Chain Risk Assessment (C-SCRA) needs of agencies in support of risk-based purchasing decisions? [Yes/No answer]

1a **If No, please provide a brief explanation.** [Short Answer]

2 **Are there any additional focus areas or questions that should be asked to help gather relevant vendor SCRI ? Please explain your answer.** [Yes/No answer]

2a **If Yes, please provide a brief explanation.** [Short Answer]

3 **Based on your initial review of the questionnaire, do you think some questions should be consolidated or removed?** [Yes/No answer]

3a **If Yes, please provide a brief explanation.** [Short Answer]

4 GSA, ITC also considered feedback from the industry to assess the impact of C-SCRM requirements on the small business community. In order to mitigate the burden of potentially negative impacts on small businesses, the GSA, ITC revised the questionnaire to better accommodate small businesses that may not have the resources for dedicated C-SCRM operations. For example, words like deploy, incident response team, reporting program, physical security team, etc., were revised or removed. Questions that focused on high-level certifications (e.g., C-TPAT, SOC 2 Type 2) that could be a disadvantage to small businesses were also removed.

If you represent a small business, do you believe there are still questions within the questionnaire that may still negatively impact you? [Yes/No, N/A answer]

4a **If yes, please provide recommendations below.** [Short Answer]

5 **If you represent a small business, do you believe a tiered assessment methodology that breaks the questionnaire into 'maturity level components' (e.g. similar to CMMC v2.0 approach) would be better suited for small businesses?** [Yes/No, N/A answer]

5a **If No, please provide any recommendations that GSA, ITC could consider for small businesses to mature their C-SCRM posture over time.** [Short Answer]

6 **If you have previously provided C-SCRM related questionnaire responses to other federal agencies as part of a solicitation, contract or task order requirement, how many have you completed over the past two years?** [Multiple Choice]

a. 1-5
b. 6-10,
c. 11-15,
d. 16 or more
e. None

7 GSA, ITC will continue collaborating with all federal agencies (i.e., NIST and CISA) in order to determine the best approach to have a common reference C-SCRM questionnaire(s), based on offering types (product, services, or both) that could be leveraged by federal agencies in their C-SCRA efforts. An additional objective is to also potentially reduce the overall industry burden associated with responding to multiple, independent government questionnaires. Vendors would only need to complete and submit the voluntary questionnaire **once**, depending on their offering type, that could then be leveraged by various federal agencies. It is anticipated that vendors will be notified on an annual basis to review and provide voluntary updates to their completed questionnaire.

Based upon your response to Question 6, what level of effort, such as the general number of hours or investment cost, did the company expend submitting the past responses? [Short Answer]

8 Would you find value in the utilization of a common C-SCRM questionnaire to provide referenceable C-SCRI responses to reduce the burden of responding to multiple questionnaires across the federal government? [Yes/No answer]

8a **If No, please provide a brief explanation.** [Short Answer]

9 **Based upon any previous experiences responding to federal agencies, what estimated level of effort (hours, investment costs) do you think it would take for vendors to complete the referenced voluntary GSA, ITC questionnaire?** [Short Answer]
Note: Please use the full breakdown of the questionnaire in the background section above as point of reference for your response based on how it may apply to your business operations. Please also identify your associated business offering type (product, service, or both).

10 In addition to responding to the voluntary questionnaire, vendors could also submit artifacts such as a C-SCRM Plan, C-SCRM Policy, and a list of suppliers.
Do you think the voluntary documents (C-SCRM Plan, C-SCRM Policy, and list of suppliers), in addition to the questionnaire, would be adequate in helping customer agencies make appropriate risk-informed purchasing decisions? [Yes/No answer]

10a **Are there any other recommended supporting documents that should be submitted to help customer agencies with their assessments?** [Short Answer]

11 GSA, ITC is exploring additional opportunities to reduce the level of effort associated with providing responses to the proposed C-SCRM questionnaire by leveraging existing investments in various industry certifications and authorizations like:

- ISO/IEC 27001, Information Security Management Systems,
- Federal Risk and Authorization Management Program (FedRAMP),
- Cybersecurity Maturity Model Certification (CMMC v2.0),
- Payment Card Industry Data Security Standards (PCI DSS), and
- SOC 2 Type 2

GSA, ITC would like to support a reciprocity approach in order to reduce the burden on industry and to streamline acquisition integrity. What considerations with industry certification(s) and authorizations, recommendations or referenceable operational examples would you suggest? [Short Answer]

Additional Questions on Post-Quantum Cryptography Readiness:

The following additional questions are included as part of the market research to identify initial industry partner IT/OT modernization efforts that are integrating Post-Quantum Cryptography (PQC) readiness and migration roadmap planning to mitigate emerging threats. Industry responses should be informed and based upon the recently released CISA, NSA, and NIST Quantum readiness factsheet (https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryp

tographic-algorithms) and current draft NIST PQC standards (FIPS 203, FIPS 204, and FIPS 205) published in August 2023.

12 **Does your company currently have a comprehensive inventory of quantum-vulnerable technologies used in current IT and OT systems and devices (custom-built or COTS) based upon assessed data criticality ?** [Yes/No Question]

12a **If Question 12 response was Yes, please provide a brief description of representative implementations of embedded cryptography within your products.** [Short Answer. If more space is needed, please include with Capabilities Statement]

13 **Does your company have a quantum-readiness roadmap that addresses your migration plans that align to the NIST defined objectives?** [Yes/No Question]

13a **If Question 13 response was Yes, please provide background information or roadmap plans on how your company is addressing overall quantum-readiness and migration to PQC.** [Long Answer]

14 **For COTS product manufacturers, System Integrators, or authorized resellers of IT/OT solutions, how does your company plan to address product updates or upgrades and/or facilitate testing for integration to enable the use of PQC?** [Long Answer]

(MORE/ RFI on Next Page)

U.S. General Services Administration Information Technology Category (ITC)

C-SCRM and Acquisition Integration

Request for Information

October 11, 2023

A. Synopsis

THIS IS A REQUEST FOR INFORMATION (RFI). This is NOT a solicitation for proposals, proposal abstracts, or quotations. The General Services Administration (GSA) Federal Acquisition Service (FAS) Office of Information Technology Category (ITC) is planning to present a voluntary Cyber Supply Chain Risk Management (C-SCRM) assurance questionnaire to vendors offering ICT products and services. The Federal Acquisition Supply Chain Security Act (FASCSA) of 2018 (part of the SECURE Technology Act of 2018) requires all agencies to assess, avoid, mitigate, accept, or transfer supply chain risks (41 USC 1326(a)(1)). A challenge for federal agencies is to identify critical risk and also use supplier C-SCRI to mitigate risk. Consistent with GSA's mission of providing a secure marketplace, we can help with the collection of Cyber Supply Chain Risk Information (C-SCRI). GSA has a role in helping customer agencies gather relevant C-SCRI to enhance customer agencies' ability to effectively assess and enhance the cybersecurity supply chain assurance related to ICT product and service offerings in the GSA federal IT marketplace.The Federal Acquisition Service (FAS)/Office of Information and Technology Category (ITC) has developed supplier assurance questionnaires to gather pertinent C-SCRI. The purpose of this Request For Information (RFI) is to seek vendor community feedback regarding the questionnaire.

B. Background

The Federal Acquisition Supply Chain Security Act (FASCSA) of 2018 (part of the SECURE Technology Act of 2018) requires all agencies to assess, avoid, mitigate, accept, or transfer supply chain risks (41 USC 1326(a)(1)). Consistent with FASCSA and GSA's mission of providing secure Information and Communications Technology (ICT) product and service solutions to agency customers, GSA coordinates the collection of relevant Cyber Supply Chain Risk Information (C-SCRI) to enhance customer agencies' ability to effectively assess and ensure the

cybersecurity supply chain assurance related to ICT product and service offerings in the GSA federal IT marketplace

C. Questions for Industry -

GSA, ITC is seeking feedback from the vendor community regarding the developed C-SCRM assurance questionnaire and initial Post-Quantum Cryptography readiness and migration roadmap planning. The questions regarding the developed questionnaire are listed above.

D. Responses Requested

All responses are requested to be provided no later than **November 10, 2023** and submitted through GSA Market Research As a Service (MRAS) only. A copy of your response will be sent to the email address provided.

E. Use of Results and Confidentiality

The release of this RFI does not guarantee that the government will, in the end, complete an acquisition or create a new SIN. This RFI is for information and planning purposes only and does not constitute a solicitation for bids, proposals or quote and is not to be construed as a commitment by the government to issue a request for proposal/quote or award of a contract as a result of this request. **This announcement is not a Request for Proposal (RFP) or a Request for Quote (RFQ).** The government will not reimburse respondents for any cost associated with information submitted in response to this request.

Any document submitted in response to this RFI that contains confidential information must be marked on the outside as containing confidential information. Each page upon which confidential information appears must be marked as containing confidential information. The confidential information must be clearly identifiable to the reader wherever it appears. All other information will not be treated as confidential.

All information marked confidential in RFI responses is only for the government's planning use. Confidential information may be reviewed by contractors providing advisory services within scope of contract, subject to a non-disclosure agreement (NDA) including but not limited to commercial or financial data obtained from or contained in contractor/vendor submitted documents and proposals. Otherwise, no information marked confidential included in this document or in discussions connected to it may be disclosed to any other party outside of the government.

For more information, please contact: gsascrmteam@gsa.gov

(end)