U.S. General Services Administration
OFFICE OF INFORMATION TECHNOLOGY CATEGORY

C-SCRM Questionnaire and Portal

May 21, 2024

ITC Office of Supply Chain Risk Management
Tom Smith, Emma Achale, Andrew Chiang

For Government Use Only

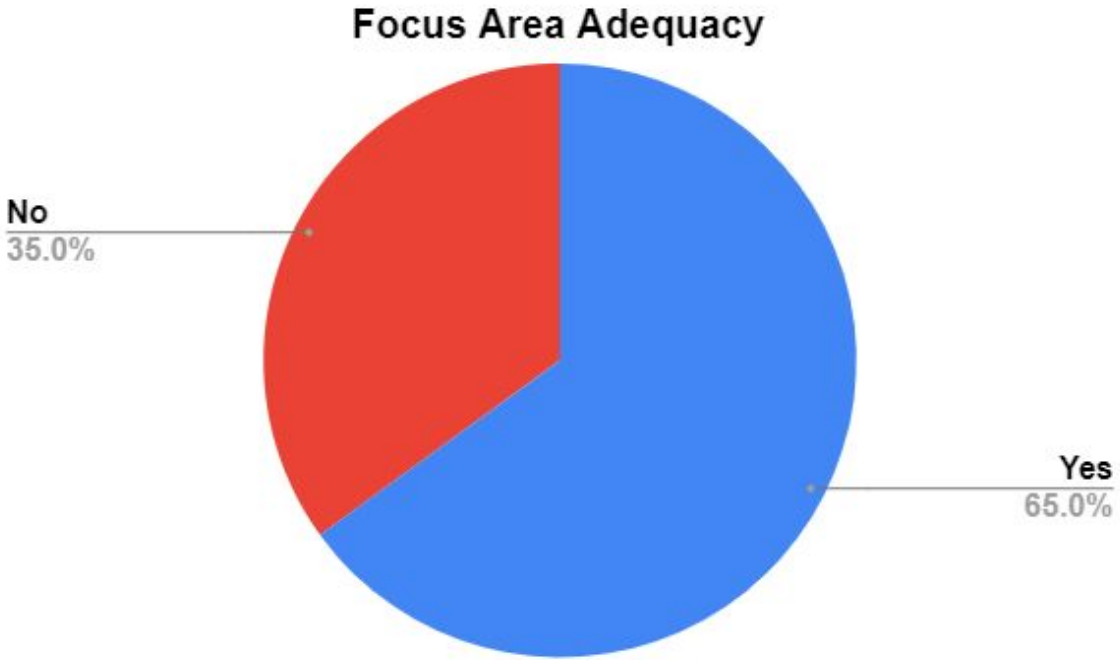
Intro

- Big thank you to industry
- Purpose of Request For Information (RFI) to gather vendor community feedback on comprehensive questionnaire
- High-level summary of industry feedback
- Updates on ITC C-SCRM Pilot program and future roadmap

Themes from RFI Analysis

- Questionnaire Adequacy:
  - Meets Supply Chain Risk Assessment Needs
  - Sufficient for customer agency purchasing decisions
- Questionnaire Focus Areas:
  - Additional focus areas recommended by vendors
- Question Removal and Consolidation:
  - Industry suggests removing or consolidating questions
- Impact on Small Businesses:
  - Preference for a tiered approach among small businesses
- Common Questionnaire Efforts:
  - Streamlining to save time and cost for vendors
- Voluntary Artifact Submissions:
  - Support for voluntary artifacts aiding risk-based decisions
- Leveraging Existing Industry Certifications:
  - Agreement to use industry certifications and authorizations

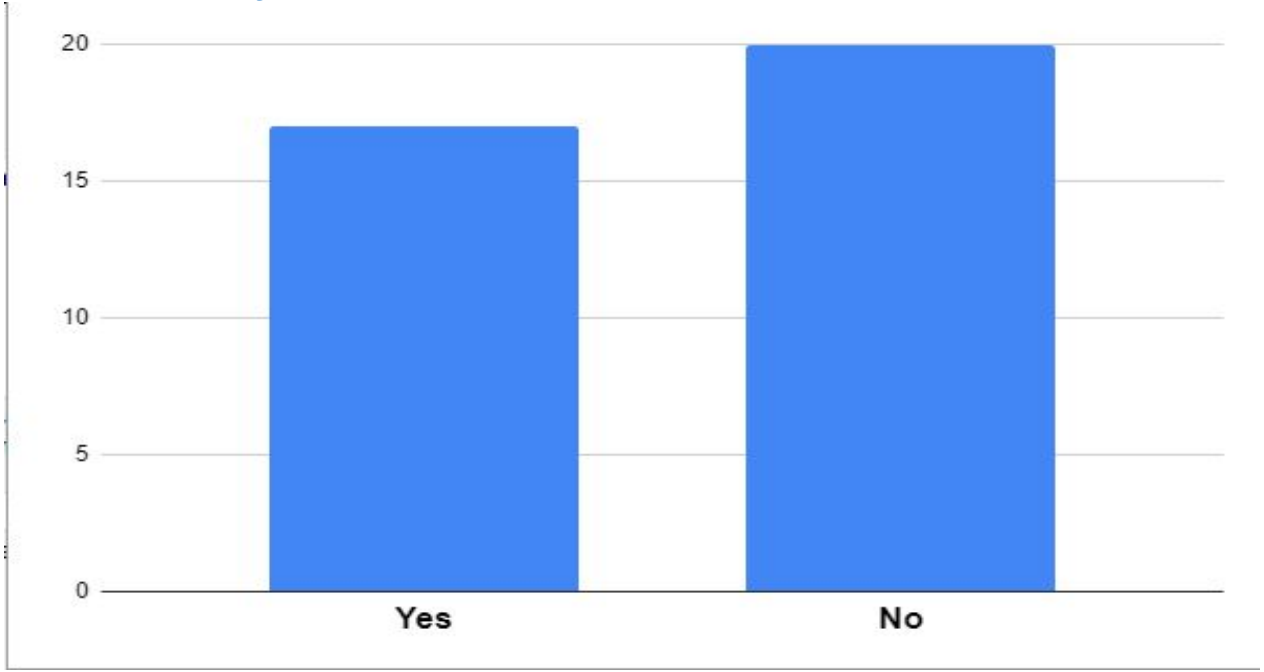
Themes in Questionnaire Adequacy - Agency Cybersecurity Supply Chain Risk Assessment (C-SCRA) Needs.



Themes in Additional Questionnaire Focus Areas or Additional Questions to Ask

No Change Needed	Additional Focus Areas
• "[Company A] considered the SCRM-AQ question set to be comprehensive and should allow GSA or other federal agencies to gather relevant vendor SCRI." • "The focus areas are comprehensive and broad as an overall template to evaluate a vendor's response and should be scoped to meet SP 800-53, SCRM Control Family requirements." • "No - we believe all questions provided cover the necessary details."	• "While addressed somewhat in the general section of the questionnaire further details on Foreign Ownership, Control, or Influence (FOCI) are warranted to give decision makers full information related to the supply chain risks and their vulnerability to foreign governments." • "Software Design & Development should be added as a section (if applicable)." • Vendor History & Reputation: What is the vendor's history in terms of security incidents? Do they have any past breaches, and how were they addressed? • Third-party Dependencies: Does the vendor rely on third-party components? If so, how do they ensure the security of these components? • "Yes - SBOMs are critical artifacts that can be used to verify how well the software supplier meets industry best practices such as NIST SP 800-218."

Are there Questions that should be Consolidated or Removed?
40 vendors surveyed; 18 Responded 'Yes', 20 Responded 'No', two did not respond)



Some responses were very specific with the exact questions that should be removed or consolidated.

Themes in Questionnaire Impact on Small Businesses

- **28 out of 40 vendors represented as Small Business.**
  - **18 of those Responded “No”; 10 Responded “Yes” to if there are still questions that will negatively impact their business.**
  - **17 of those Small Businesses also responded that a tiered Approach (e.g., CMMC) would be better suited for their business**

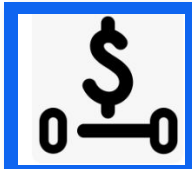
Themes in Efforts and Having a Common Questionnaire

Past Two Years

- 67% of vendors have submitted a questionnaire within the past two years
- ~20-30% of vendors submitted between 4-10 questionnaires within the past two years
- 12% of vendors submitted > 10 questionnaires

Past Response Time

- Very broad range: 1 - 200 hours
- No response from 28% of vendors



Past Cost Range

- Few broad responses
- Most response were $12K+

Out of 40 responses, 90% vendors responded yes to finding value in the utilization of a common C-SCRM questionnaire.

Themes in Level of Effort Needed to Complete the ITC Voluntary Questionnaire

- 4 [1-4 hours]
- 2 [8-10 hours]
- 2 [20-24 hours]
- 5 [40-80 hours]
- 3 [80-120 hours]
- 1 [40-200 hours]
- 1 [1-2 weeks]
- 13 blank or answers which did not accurately respond to the question.
    - *Some noted difficulty in responding as the questions were not fully aligned to a framework. Some noted the additional time would be for developing the related documentation.*

Themes in Leveraging Existing Industry Certifications

Industry recommended different industry certifications that should be considered.

The industry certifications were widespread. However, the respondents were consistent in their response that the requirements should map to a standard.

Most Common: NIST SP 800-53, FedRAMP, ISO/IEC 27001, CMMC v2.0, PCI DSS, and SOC 2 Type 2

Themes in Voluntary Artifacts for Vendor Submissions

Below is a breakdown of responses related to if in addition to the questionnaire, the C-SCRM Plan, C-SCRM policy, and a list of suppliers will be beneficial for customer agencies to make appropriate risk-based purchasing decisions.

- **73% responded Yes**
- **25% responded No**
- **1 blank**

Post-Quantum

01	**NO: 73%** **YES: 27%**	• Have a comprehensive inventory of quantum-vulnerable technologies used in current IT and OT systems and devices (custom-built or COTS)?
02	**NO: 56%** **YES: 44%**	• Have a quantum-readiness roadmap that addresses your migration plans that align to the NIST defined objectives?
03	**MIX STRATEGIES**	• Strategies by vendors who said “Yes” to being ready: Assessment | Education | Testing and integration | Quantum-Resistant Algorithm Selection. • Some vendors have detailed plans for product updates, upgrades, and integration testing for quantum-resistant algorithms.

Key Takeaways

- More actions in FY24 and FY25
- Constant improvement is key
- Ensure we are leveraging certification (i.e., CMMC)
- There is really a need for a common questionnaire
- Burden is a factor: small and large businesses
- A portal will benefit our vendors and agencies

GSA ITC FY25 C-SCRM Pilot (Overview)

- Issue
- Journey
- Concept
- Need
- Goal
- Solution

GSA ITC FY25 C-SCRM Pilot (Next Steps)

- Brainstorm and design
- Business case and proposal
- Funding request
- Approval and implementation

GSA ITC FY25 C-SCRM Pilot (Collaboration)

- Partnership with government agencies
- Sharing C-SCRM lessons learned
- Participate in the proof-of-concept
- Soft Launch when ready
- Continual improvement

GSA ITC Contact Information

- Andrew Chiang, Technical Advisor, Supply Chain Risk Management Office (SCRM), andrew.chiang@gsa.gov
- Emma Achale, Branch Chief, Supply Chain Risk Management Branch, emmanuella.achale@gsa.gov
- Tom Smith, Deputy Director, Supply Chain Risk Management Office, thomasl.smith@gsa.gov
- Matt Jones, Senior Director, Supply Chain Risk Management Office, matthew.jones@gsa.gov

Questions?