interos

April 25, 2022

RFI Response for 87 FR 9579

Submitted Via Email to *CSF-SCRM-RFI@nist.gov*

Please find below Interos' response for **RFI 87 FR 9579**.

Use of NIST Cybersecurity Framework

NIST Question 2: Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?

The NIST standard improves communication since all parties refer to the same standard and terminology. Concerning supply chain management, Interos believes that there should be continuous monitoring of suppliers for multiple risk categories not just cyber. Other risk categories such as financial risk and sanction violations should be included in the NIST risk assessment as the significant events create an environment for cyber breaches.

Cybersecurity breaches follow the same risk assessment NIST has always had. But including sanctions or restriction violations with a yes/no rating on the suppliers provides a more holistic picture of the supplier and if they are compliant with US laws. Financial risk accounts for sales of a firm and solvency so they can employ the right cyber security protections. A relevant metric would be a pre-and post-assessment of the number of suppliers monitored and how well they are being tracked. In the longer term, one should look at the overall health of the supply chain and revue the trends in the various monitored risk categories.

NIST Question 3: Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

Interos does not believe the NIST framework is more intrusive or burdensome than other frameworks. However, supplier onboarding is typically done in manual operation with the completion of forms, etc. This can be not very easy for suppliers and time-consuming for the purchaser. Standardizing supplier onboarding with an external assessment of risk factors would simplify initial supplier assessments and standardize the entire process.

NIST Question 4: Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.
Interos believes the NIST framework should have a standardized supplier monitoring and assessment. Most supplier vetting is done initially and then with annual surveys. Interos thinks that in the modern fast-changing world, surveys are no longer acceptable and that NIST must adopt a continuous monitoring posture.

NIST Question 5: Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.
If NIST were to adopt more modern supply chain security practices such as standardized supplier assessment using public information and continuous monitoring, Interos believes this could greatly simplify some current procedures, such as sending extensive surveys to suppliers and waiting for their completion and return. This would enable suppliers to streamline their processes and reduce reporting costs, while improving the quality of the data used in the assessment. This would effectively supersede existing processes while significantly increasing useability.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

Interos believes that adding continuous supplier monitoring for multiple risk factors would improve the NIST format. Traditionally the security organization cared about cyber risk scores, the purchasing group about the supplier's financial score and the legal/compliance team was concerned about sanctions or restrictions. These factors are assessed in different ways by different groups and often siloed from each other. Interos believes knowing the overall health of suppliers is critical to preventing supply chain cyber events or forced supplier replacement due to financial or sanction issues. This assessment should be done continuously in a standardized manner that is not burdensome to the supplier.

NIST Question 7: Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include:

- **Risk management resources include the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).**
- **Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.**
- **Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.**

Interos believes that the continuous monitoring of suppliers for multiple risk factors is an appropriate addition to all-risk frameworks. Every organization should be aware of its supply chain and make decisions about onboarding/using/replacing suppliers in all industries and environments in a proactive manner. This applies to all frameworks that use external suppliers to support organizational operations.

Including comprehensive monitoring and assessing, suppliers would be appropriate to add to Enterprise risk as in NISTIR 8286. Assessing software supply chain suppliers and IoT devices would be right in trustworthy development processes, and it should be included in cyber-security education. Even selecting schools or partners for cyber education should use a proper vetting program to prevent partnerships with poor providers.

Supply chain issues affect every organization and program and should be the front center of any risk and controls efforts.

NIST Question 9: There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience, can promote innovation and competitiveness while enabling organizations to more efficiently and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?

Interos would expect a suggested approach to continuously monitor and assess the supply chain for multiple risk factors would be entirely applicable to internal standards and have the same value.

Cybersecurity Supply Chain Risk Management

NIST Question 11: National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the most significant challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

Interos believes the biggest challenge is to provide a consistent, comprehensive approach that is not too burdensome on the purchaser and the supplier. Traditional systems of periodic surveys are ineffective because they enable gaps of time where vulnerabilities exist and are a drain on suppliers. A single consistent method of assessment would reduce these burdens.

NIST Question 12: Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

Interos approach provides a Software as Service (SaaS) platform to map and monitor the extended supply chain. Our system uses a data lake of 400 million entities with supplier-buyer relationships gathered from public and commercially available sources. We also import about 100,000 + intelligence feeds to apply to these entities.

Interos uses artificial intelligence and machine learning to build the relationships and then apply the appropriate factors to each entity. We then use a comprehensive risk assessment to apply six major risk categories: cyber, financial, sanctions, geopolitical, operational, Environmental, Social, and Governance (ESG) risk factors to each supplier. The Interos approach uses a single source of truth for the organization where they are cyber, procurement, legal, sustainability teams, etc., to apply a consistent, standardized approach to supply chain security. Using a single platform would reduce suppliers' burden on complying with reporting requirements.

NIST Question 13: Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?

Interos believes there is a significant skills gap in cyber and risk professionals in the supply chain. We propose that additional training be provided, and the supply chain added to the industrial control system and software supply chain education.

NIST Question 14: Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.
Interos believes that supply chain suppliers' active monitoring and assessment should be continuous, use multiple risk factors (cyber, financial, and sanctions), and cross-organization. They should be done in a standardized manner that is not burdensome to the suppliers themselves. This effort will prevent supply chain attacks and disruption, which will enable organizations to be more efficient and save money and staffing hours while improving overall performance.

Yours Sincerely,

Sara Akbar
Sr. Director, Government Affairs
[redacted]