PUBLIC SUBMISSION

As of: 4/27/22 6:41 AM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2f-10fa-zbsg
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0047
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: American Petroleum Institute

General Comment

The American Petroleum Institute (API) offers the attached comments on the National Institute of Standards and Technology's (NIST) Request for Information; Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management, Docket Number: 220210-0045. API is a national trade association that represents approximately 600 members involved in all aspects of the oil and natural gas industry, including producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry. API members are deeply committed to safe, secure, and environmentally responsible operations which eliminate or reduce potential risk to the public, as well as employees, contractors, and operations.

Attachments

API Response to NIST CSF RFI 25APR22 FINAL

NIST CSF RFI – Docket Number: 220210-0045

Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

The American Petroleum Institute (API) offers the following comments on the National Institute of Standards and Technology's (NIST) Request for Information; *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management,* Docket Number: 220210-0045. API is a national trade association that represents approximately 600 members involved in all aspects of the oil and natural gas industry, including producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry. API members are deeply committed to safe, secure, and environmentally responsible operations which eliminate or reduce potential risk to the public, as well as employees, contractors, and operations. Safety and security are key elements in all operations, and we continue to work with our federal partners to ensure we are operating in a manner that secures our networks, operations, and assets, and improves our country's and our critical energy infrastructures' ability to thwart cyber compromises, in whatever form they may take.

1. The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.

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?

Answer to Questions 1 & 2

API members, from its development, have supported the NIST Cyber Security Framework's intent and usefulness. API member companies have used the Framework as the foundation for their cyber security programs, as core principles for the execution of those programs, and as a tool to assess the return on investment of various cyber security practices and programs. The Framework has also been used as the basis or guiding principle for industry standards, including API's STD 1164, *Pipeline Control Systems Cybersecurity.* The industry outlined the ways in which the oil and natural gas industry has adopted the tenets of the Framework in our 2018 report, *Defense-in-Depth: Cybersecurity in the Natural Gas and Oil Industry.* According to the report:

> "Natural gas and oil companies implement cybersecurity programs that comprise many components. Companies often frame these components through the lens of the NIST

> Cybersecurity Framework (CSF), a voluntary framework intended to provide a common language organizations can use to assess and manage cybersecurity risk.”

This graphic from the report illustrates how the industry has conceptualized the Framework:

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).

While many API members have utilized the Framework, there are improvements that could be made to make it easier to adopt. First, some of the references to controls can be very vague and could use more context to apply them better to the assets.

A common starting point for ingesting the CSF within a company is to map the subcategories to standards already in use. The informative references on the surface would seem to do this but the informative references are more suggestions than mapping. Companies using the informative references as a mapping to the CSF quickly find themselves in a quagmire as the standards tend to map on a many-to-many basis.

The CSF is flexible and there is plenty of content but it can take significant resources to determine what needs to be done and by whom. Profiles can help but these have not been developed for all facets and some which have been developed can themselves be difficult to understand.

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.

API members have noted several items that could be added, changed, or removed. While the Framework has training plans and awareness training for general employees, there is nothing included to train the cybersecurity workforce and NIST should add this guidance. NIST should add cybersecurity strategy implementation guidance, as well as System Development Life Cycle guidance. NIST should also consider incorporating guidance for open-source software elements. NIST should consider whether guidance should be included for artificial intelligence modeling. Lastly, NIST should consider how to incorporate guidance for how to manage end of life cyber security requirements.
Other additions:

- Provide advocacy to influence legislation and regulation and comply with applicable laws and regulations. There is a subcategory covering understanding and managing legal requirements which might include advocacy but it might be better to explicitly call this out.
- Establish requirements to close assessed gaps (from Conformance Assessments, IRM Plans, Vulnerability Assessments, and Cybersecurity Exercise Program). The text of the CSF talks about establishing a current and target profile and addressing the gaps but there is nothing specific in the CSF to execute this function.
- Determine which manual processes require automation. Current CSF does not address automation.
- Conduct strategic research (near and long term) on new security technologies and new technologies that may have security ramifications. The CSF covers the assessment of risk but is missing some of the other components of building a strategy like identifying new technologies.
- Develop and Execute Strategy, Asset Plan & Architecture. Current CSF does not address building a strategy or a cybersecurity architecture.
- Risk management strategy needs to be fleshed out. Proposed extensions
    - Manage risk assessment and exceptions process

    - Plan for processes to assess implementation of the foregoing organizational measures and controls
    - Develop Risk-Based IRM Plan
    - Technology risks are understood and documented
- The CSF needs to accommodate DevSecOps.   This would include more explicit references to Secure Software Development.   This may lead to deleting "PR.DS-7: The development and testing environment(s) are separate from the production environment" as with DevSecOps, there is a blurring of development and production.
- New subcategory for Protect – Maintenance: Renew, retire, or replace technologies according to plan and in coordination with analysis and operational teams
- New subcategory for Response – Analysis: Provide Forensics Expert Consulting

Additionally, the Supply Chain subcategories in Identify should be moved to proper areas of the CSF. ID.SC-1 and ID.SC-2 should be under Risk Management or Risk Assessment. ID.SC-4 and ID.SC-5 should be in protect

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.

Major structural changes (removing functions or moving large number of categories from one function to another) would disrupt the history of benchmarks and other items based on the existing CSF.   If categories or subcategories were moved intact, one might be able to manage this change but could manage this.   If the subcategories were split or combined, then users would lose the historical context.

6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.

API members support the idea that the profiles are the best ways of slicing the framework and that the existing profiles are necessary and potentially more may be needed. Profiles provides views as to how the CSF may be applied to specific industries or business practices and therefore make it easier to deploy the CSF (and therefore make it more useful)

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 such as 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.

API does not have suggestions for these resources.

8. Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or

integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?

API would encourage NIST to align with ISO standards when appropriate, and potentially create a taxonomy or glossary to better understand where there are common terms or concepts. NIST should also review common frameworks used in other countries, and other types of frameworks, such as automated controls frameworks, cloud frameworks, and the MITRE ATT&CK matrix. NIST should also encourage more organizations to provide mapping and alignment from standard to standard to help operators as they attempt to implement multiple frameworks. A major benefit of us would be for regulators to create profiles (as the Coast Guard did) or map their regulations to the CSF. Use of the CSF avoids the creation of too prescriptive, one-off regulation and makes it easier for the regulated companies to implement (comply) as the regulation would map to something (CSF) already in use in the company.

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 easily 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?

To potentially expand global use of the framework, NIST should consider the requirements that exist in other countries and how does the Framework map to others. NIST should also consider how the Framework can be substituted for certification. For example, if you are certified to ISO, that certifies or gets you some certification for NIST or vice versa.

10. References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.

API members encourage NIST to send out a draft with a bulleted list of references for industry users to review and potentially add to.

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest 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?

API members encourage NIST to perform an audit of all federal government supply chain initiatives to better understand where there is overlap, where there may be gaps, and what are the most significant challenges to the success of any of those initiatives. NIST can then shape its own program to take advantage of and harmonize the others.

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.

API members would point NIST to the collaborative project that was developed with the Linking the Oil and Gas Industry to Improve Cybersecurity program (LOGIIC), an ongoing collaboration of oil and natural gas companies and the U.S. Department of Homeland Security, Science and Technology Directorate. In 2021, LOGIIC conducted a study to understand how Software Bill Of Materials and other vendor capabilities can be used to manage cybersecurity risks to industrial control systems (ICS) software that may be introduced from third-party components that are part of vendor solutions. More can be found here.

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?

The preponderance of cybersecurity supply chain risk management guidance and resources makes it difficult to determine what gaps, if any, currently exist. NIST should consider how all of these resources align to assist users in their application cyber security supply chain risk management.

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.

API members encourage NIST to consider accounting for Cybersecurity Supply Chain Risk Management Guidance in the Framework, but a separate profile might be able to demonstrate what is in the pieces of supply chain that go in each category. NIST may also consider creating a profile based on the Framework that applies to supply chain and uses references to other supply chain tools and guidance.

Should you have any questions, please feel free to contact me at [redacted] or [redacted].

Thank you,

Suzanne Lemieux

Director, Operations Security & Emergency Response Policy

Corporate Policy

o: [redacted]

m: [redacted]

e: [redacted]

[redacted]