AGA
American Gas Association

April 25, 2022

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

RE: NIST Cybersecurity RFI – NIST Evaluating & Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management [Docket Number: 220210–0045]

On behalf of the members of the American Gas Association (AGA), Association of Oil Pipe Lines (AOPL), American Public Gas Association (APGA), and Interstate Natural Gas Association of America (INGAA), please accept the following responses to the NIST Request For Information published in the Federal register on Tuesday, February 22, 2022.

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

Kimberly Denbow | Managing Director, Security & Operations
American Gas Association
400 N. Capitol St., NW | Washington, DC | 20001
[redacted]

AGA, AOPL, APGA, and INGAA appreciate the opportunity to provide feedback on the National Institute of Standards and Technology (NIST) Request For Information (RFI) dated February 22, 2022 to improve the ''Framework for Improving Critical Infrastructure Cybersecurity'' (CSF) and a variety of existing and potential standards, guidelines, and other information relating to cybersecurity in supply chains. Our trade associations represent major aspects of U.S. energy pipeline operations, including regional and local natural gas distribution pipelines, natural gas transmission pipelines, hazardous liquid pipelines, and municipal natural gas systems, which all serve customers safely and reliably throughout North America. For nearly a decade, we have worked along-side NIST promoting the adoption of the CSF across government and owner/operators. We appreciate the ongoing effort by NIST to support a broad, cross-sector cybersecurity framework to reduce cybersecurity risk to critical infrastructure.

Natural gas and hazardous liquid pipeline operators have reviewed the NIST RFI and generally feel the CSF is a valuable tool that has been widely adopted by many companies and partners. It is a risk- and performance-based framework critical for success of management of cybersecurity vulnerabilities. It is important for energy pipeline companies to have the latitude to balance safety and operational risks as driven by an evolving cyber threat landscape.

Recognizing there are areas for improvement, as outlined below, we caution against an overhaul of the CSF. The language has become a common lexicon for many – interwoven into our cyber fabric – and has been built into many corporate processes and other frameworks for information technology (IT) and operational technology (OT). The overall structure is solid, but as it expands, it becomes more complex. It should be kept at a concise high level to continue to provide flexibility. The overall CSF may be pruned down in some areas to ensure a well-balanced document. The comments below provide specific examples of what works well and what can be updated.

Use of the NIST Cybersecurity Framework

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.*

USEFULNESS OF FIVE FUNCTIONS:
The NIST CSF can be leveraged by an organization to internally measure its security practices against a target state to help it elevate the security posture from both an administrative as well as technical perspective. The CSF provides a common framework across all industries, is reproducible, and can be referenced and adopted by third parties. The 98 controls in the CSF are used as a baseline upon which other standards are applied.

The CSF has become an integral part of the cybersecurity practitioner's lexicon for describing cybersecurity capabilities. The five functions in the CSF are a foundational communication tool for technical and non-technical audiences. All audiences can conceptually understand the five functions and how actions/investments tie back to support one or more of the functions, while the more technical audience can progress further to the other aspects of the CSF such as the categories and subcategories.

The CSF can be molded to promote conversation across different types of organizations (i.e., state, federal, contractors, cross-industry) as well as between practitioner and cybersecurity solution providers. For example, the CSF provides a good baseline for discussions between the operator and the state energy official.

The five functions of the CSF are applicable regardless of organization sector, size, or structure. For example, AGA member energy utilities have adopted the AGA Commitment to Security, which provides actions broken into the CSF five functions. The five functions provide structure through a common language to discuss cybersecurity capabilities, programs, and practices. The CSF is a tool that can be used to demonstrate and communicate progress or need for further actions in the five functions. Maturity can be shown through a comparison of the current state and of the desired state (profile), which helps link investments/activities needed to achieve the desired outcome.

The common language and structure that comprise the CSF has been woven into existing industry standards and government programs, e.g., *API 1164 3rd edition Pipeline Control Systems Cybersecurity* and Department of Energy Oil and Natural Gas (ONG) Cybersecurity Capability Maturity Model (C2M2) used in the energy sector.

AREA FOR IMPROVEMENT:
The CSF subcategories could be more inclusive to address NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity. NIST should avoid adding to the five functions. Additions/augmentations should fit within the existing functions.

Use of the NIST Cybersecurity Framework

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?*

COMMUNICATION:

The CSF helps bridge all levels of cybersecurity understanding regardless of technical acumen and background of the audience. The common language of the CSF can be molded to promote conversation and align expectations within a single organization and across different types of organizations (i.e., state, federal, contractors, cross-industry). For example, the CSF provides a good baseline for discussions between the operator and the state energy official. The CSF has become an integral part of the cybersecurity practitioner's lexicon for describing cybersecurity capabilities. All audiences can conceptually understand the CSF, while the more technical audience can progress further to the next level. For example, the *Identify* function supports strong cybersecurity governance, policies, and procedures; detects gaps in those policies and procedures; and is easy to communicate at the board-level. The CSF also helps inform an organization's risk register and roadmaps. Given that the CSF is internally benchmarkable, an organization can demonstrate improvements across the controls and, as such, can help shed light on adjustments needed to the organization's roadmap. Owners/operators use the CSF for internal communication and communication with regulators.

Some owner/operators believe the CSF has not been adopted by supply chain partners nor insurers, who tend to focus more on practices rather than the CSF 'tier' of their service/product. The value of incorporating the CSF into discussions with supply chain partners and insurers will remain minimal until those groups build CSF into their programs. There is value in having a list of capabilities (or even the subcategory of the CSF) the solution/product supports. The NIST 800-53 may be leveraged with CSF to satisfy to this. Within the energy industry, tying the NIST CSF to the controls in DOE C2M2 would be a way to improve communications with these entities as it relates primarily to expectations for assessments.

RISK MANAGEMENT & ASSESSMENT:

Risk appetites vary within a single organization as well as across different organizations. The wide applicability of the CSF is attributed to its flexibility to be molded to the risk profile at hand regardless of the individual organization size, cyber maturity, or risk tolerance. The CSF tells one what needs to be done, not how to do it – this allows the operator to determine the best approach for the operations and for the organization's risk appetite. By not being overly prescriptive, the CSF does not become dated, which is particularly important given cyber is a constantly evolving risk.

While many organizations rely on the CSF as valuable for addressing risk, others leverage the CSF to self-identify gaps, which are then evaluated in a separate process independent of the CSF. This bifurcation has merit among organizations that build other factors into their assessment, especially if risk alone does not get the organization to its desired security state.

Two points worth noting:

- Smaller organizations may benefit from a lighter version of the CSF – while maintaining the five functions – given the full CSF may not be applicable. This is particularly true when such organizations leverage the CSF as a set of “best practices” because they do not have a mature risk management process to evaluate gaps in terms of risk.
- The CSF must remain technology agnostic; allowing the operator to determine the best application for achieving the function. For example, *Identify* is about knowing what one has; the path to achieve that should not be defined nor limited by a government-assigned technology.

METRICS:

The intent of the CSF is broad application across the 16 critical infrastructure sectors (at the time of development, there were 18 critical infrastructure sectors). Detailed metrics has been and continues to be the wrong question for the purpose of the CSF. Metrics should be around adoption of the CSF by an organization and whether that adoption has helped the organization improve its cybersecurity program and capabilities focused on reducing risk. Metrics should also be the incorporation of the CSF into industry standards, practices, etc. Metrics focused on specific control objectives inside the CSF defeats the broad applicability and flexibility that make the CSF valuable. Additionally, NIST could publish a practice reporting document or update their Performance Measurement Guide for Information Security.

Use of the NIST Cybersecurity 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).*

That which may be viewed as the greatest strength of the CSF – its flexibility – may also be perceived as its greatest challenge. The quantity of control objectives and complexity of the language can be intimidating for small to medium size organizations that may lack the expert assistance or investment resources. By making more training and tooling available to supplement the CSF, all interested audiences are afforded the opportunity to employ the CSF as intended. Training will help operators distinguish among the CSF, the Special Publications, and the Informative References. While the NIST website and resources demonstrate the CSF can be used in some capacity by organizations of all sizes, the online learning content page should be more user-friendly and intuitive to navigate.

Not all organizations have the resources to map controls to the CSF. Mapping to other control frameworks, e.g., DOE C2M2, COBIT, NERC CIP, can become complex and difficult to manage when supporting frameworks change.

There remain challenges in mapping more technical controls and in retrofitting other best practice controls into the CSF. Furthermore, issues exist for multinational companies or for companies that use international vendors when the CSF is not recognized outside of the United States. Similarly, other compliance programs, such as the U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC), do not align completely with the CSF, which presents difficulties for defense contractors.

Use of the NIST Cybersecurity Framework

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.*

ONLINE LEARNING:
The online learning content page should be more user-friendly and intuitive to navigate, including a simplified explanation of where to begin and how the standards work to supplement CSF. For example, utilizing tiers can be challenging, either because of misunderstanding of their use or difficulty to tie them back to categories, subcategories and reference standards. NIST controls should be supported by a separate Implementation Guidance document that could list general recommendations that can be broadly applied. i.e., do not list prescriptive requirements.

MAPPING:
NIST's references and crosswalk with the NIST 800 series (e.g., 800-53) guidance is helpful for providing detailed controls to help achieve the objectives. Sector Risk Management Agencies can be encouraged to work with their critical infrastructure sectors/subsectors to map the CSF to industry frameworks and standards similar to what DOE did with the Energy Sector for the C2M2 and what the Pipeline Subsector did with its development of API 1164 3rd edition. Such mappings can be too resource intensive for individual organizations to efficiently develop and effectively maintain.

SCORING:
NIST should educate organizations to apply the CSF accordingly as a tool for subjective identification of internal gaps but not as a tool for comparing scoring with other organizations. Scoring and consequentially comparing companies or industries with the tool can lead to the misapplication and misinterpretation of results, e.g., low scores in one organization as compared to another could be misinterpreted as low levels of security. CSF is good for supporting internal comparison of an organization of where it is at with respect to the target in CSF the organization has chosen to attain. Since organizations can select what to include in their target profile, the results are not an objective assessment for external comparison.

PROFILE TEMPLATES:
Functions, categories and subcategories are helpful elements. The inclusion of profile template(s) would be beneficial, especially for the small and medium size organizations which may need to rely on templates from third party vendors. It would be beneficial to have a reference profile template, while acknowledging organizations still have flexibility to use their own profile creation approach. Improvements could be made to the guidance on how to use the CSF more broadly and for purposes of assessments to address challenges relating to how third parties interpret the CSF. Further, the CSF should move to address third party risk and be kept up to date at a pace that meets those of the updates to its referenced standards.

ADDITIONAL SUBCATEGORY:
An additional consideration is the creation of a subcategory around consequence to the attacker under the *Respond* function. This consequence should be a legal federal response from the judiciary that codifies the federal government's responsibility to support private sector and prosecute cybercriminals.

Use of the NIST Cybersecurity Framework

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.*

Backward compatibility is valuable to reducing implementation costs. In cases where change may be necessary, consider flexibility in implementation as well as implementation in stages to ensure organizations understand the sequence and timing of events.

Any major changes to the CSF will have negatively cascading impacts on organizations that have implemented and built internal programs around the CSF. In particular, there would need to be remapping and the reform of government as well as corporate programs that are based on the current CSF. The five functions of the CSF were intentionally selected since they are timeless, fundamental, and can adapt with changes in technology and threat landscape.

Although the CSF is intended to be a voluntary framework, a multitude of organizations and government agencies has aligned with it. Overarching changes to the CSF would require an immediate rework by those organizations, which may either drive them to move away from the CSF; to continue to use the older framework; or to redirect limited resources, including staff time and finances, to adapt to the new structure. Such redirection would be counterproductive to the objective of improving security.

Core functions should remain stable and unchanged, if possible. Category and subcategory changes are disruptive but are less likely to impact usability and compatibility. It is important to maintain mapping to supporting controls from other frameworks like NERC CIP, COBIT, etc. If CSF changes, then a remapping needs to happen. This is a lot of work for smaller organizations and has curbed some operators' adoption beyond the original release.

Use of the NIST Cybersecurity Framework

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

Existing assessment and maturity models offered by NIST could be more thoroughly mapped to the CSF, and training resources, e.g., an online or software-based tool to use in conjunction with existing mappings, could be improved. It is important to ensure clarity in the relationships between guidance from NIST and materials produced from federal and state governments. Without clear relationships and hierarchy between materials created, the cybersecurity guidance space becomes crowded and potentially duplicative, and the relevance of the CSF is overshadowed by cyber regulations, especially if the regulations are not built on the CSF. Two timely examples, include the 2021 TSA Pipeline Security Directives and the first draft CISA *Common Baseline Industrial Control System Performance Goals*, which were not structured to align with the CSF. Two examples of resources effectively built on the CSF, include the TSA *Pipeline Security Guidelines (March 2018 (with Change 1 (April 2021))* and the API 1164 3rd Edition*, Pipeline Control Systems Cybersecurity Standard*.

Having NIST create templates, which can be used to create profiles and assessments against the profiles, would be beneficial for all audiences. Smaller companies may find it more useful to create a more risk-based tool and mapping to compliance-based frameworks. Such organizations tend to leverage best practices; so a 'best practices' version (rather than risk version) that lays out a priority of practices may more efficiently help small organizations manage leading risks.

Implementation guidance relative to the various Special Publications (SPs) would be beneficial. At present, moving from one document to another is cumbersome and challenging. Additionally, some elements or categories are highly prescriptive and do not leave flexibility for alternate controls. One such example is PR.IP-1 which, prescribes maintaining and protecting a hardened baseline image. Hardening can alternatively be performed by using the latest image and hardening via GPO configuration.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

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:*
    a. *Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286).*
    b. *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.*
    c. *Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.*

RELATIONSHIP BETWEEN CSF AND RISK MANAGEMENT RESOURCES
The CSF was developed and socialized to be the lexicon for use by government and critical infrastructure. Aligning the resources listed above to the language in the CSF is not only beneficial but essential. The seven steps identified in the NIST Risk Management Framework (RMF) are helpful guidance and provide a guideline to ensure no gaps in an organizations process.

Whereas the CSF is the foundation and the “Policy” piece that identifies issues and the appropriate scope for cybersecurity programs, the NIST Risk Management Framework, the Privacy Framework, and other resources are used at the next level of complexity, much like a prescriptive “Standard”. A resource like a NIST Interagency or Internal Report (NISTIR) would then be at an increasingly granular “Procedure” level to achieve what is required at the “Standard” level. All these resources are built <u>on</u> the CSF, not vice-versa.

Changing these more detailed resources to reference the CSF more congruently would be useful, including up-front, updated guidance on implementation of these resources alongside NIST CSF. On the flip side, a substantive change in the CSF to align with these other resources is illogical and comparable to changing out the engine and body of a vehicle to accommodate the tires.

It’s worth noting the resource materials should be simplified (too many pages). There is minimal “out of the box” alignment or integration. For example, RMF in its entirety is not practical for smaller organizations or private organizations. The RMF needs to be streamlined significantly for small teams. Further, control references besides NIST 800-53 would be needed.

RELATIONSHIP BETWEEN CSF AND TECHNOLOGY RESOURCES
Subcategories in the CSF could better address the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity.

RELATIONSHIP BETWEEN CSF AND WORKFORCE MANAGEMENT RESOURCES
It is unclear how NICE and the CSF would need alignment. They have value independent of one another.

Relationship of the NIST Cybersecurity Framework to Other Risk Management 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?*

COMMONALITIES/CONFLICTS – CSF AND OTHER VOLUNTARY, CONSENSUS RESOURCES
The oil and natural gas industries intentionally aligned with the CSF when developing its latest version of industrial control system cybersecurity standards for pipelines (API 1164 3rd edition).

COMMONALITIES/CONFLICTS – CSF AND CYBER MANDATES/RESOURCES FROM GOVERNMENT
There are notable commonalities between the CSF and *TSA Pipeline Security Guidelines* and DOE ONG C2M2, which were developed prior to the CSF but were reconstructed around the CSF following its release in 2014. Some mandates are more prescriptive, e.g., NERC CIP and TSA Pipeline Security Directives, while others are more flexible and let the organization choose how best to achieve the security objectives, e.g., COSO, SOX.

Industry and cyber practitioners have bought into using the CSF as a common lexicon. However, the federal government continues to be inconsistent with applying the CSF when defining guidance, mandates, and other resources, e.g., first draft of CISA Common Baseline Performance Goals and TSA Pipeline Security Directives. One way to improve alignment would be to have a common framework for all compliance regulatory agencies.

IMPROVE ALIGNMENT/INTEGRATION – CSF WITH OTHER FRAMEWORKS SUCH AS INTERNATIONAL
Given the CSF is not internationally-recognized, the alternative may be to use the Center for Internet Security (CIS) Controls version 8, which maps effectively to other standards, including API 1164 3rd edition and IEC 62443.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

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?*

International companies might be more apt to use ISO standards. It's worth recognizing that ISO is not free and located behind a paywall.

The CSF is conceptually strong, flexible, and complimentary, which serves the needs of domestic organizations. NIST should ensure the CSF continues to be available at no cost and easily assessable.

International adaptations of the NIST CSF typically either align directly with the NIST CSF or add additional controls. Remaining flexible and less prescriptive is critical to international adaptability and usability.

CSF should remain at the current level, which allows it to withstand the evolving threat landscape and technological changes. Minimize annual updates. Constant change to the framework will be expensive for users and may limit their progress in implementation; stability will allow operators to work towards it.

Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

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.*

- The Institute of Internal Auditor's (IIA) Three Lines of Defense Model
- DOE C2M2
- API 1164 3rd edition
- *TSA Pipeline Security Guidelines* and Pipeline Security Directives
- NERC CIP
- NIST SP 800-82, Rev. 3

Cybersecurity Supply Chain Risk Management

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?*

The NIICS could provide value addressing supply chain software risk as it relates to software bill of materials (SBOM), hardware bill of materials (HBOM), and software as a service (SaaS) BOM. Additionally, the creation of a certification process or defined assurance levels, or standards for vendors and software would be beneficial to industry.

There needs to be a mechanism by which the organization can:

- ensure the supplier is in compliance with agreed upon cyber provisions, i.e., having a standard or baseline set of qualifier requirements for suppliers to comply with,
- ensure software that is purchased/installed meets the cyber integrity provisions, i.e., having a standard set of disclosures a supplier must make, e.g., identify applicable data centers hosting their software; geo location of where software was developed and supported from; build of materials of all software used in the making of the product, including open source,
- ensure appropriate level of supplier product/service redundancy, i.e., resilience.

A certification process/standard may be able to push vendors at a higher level to promote better cybersecurity practices. Individual companies are limited in what they can do in their assessments and the influence that they have with their suppliers. Individual organizations can and do employ cyber provisions in their procurement language. However, making this type of certification obligatory – whether through the government or third-party assessor – would be helpful to the larger critical infrastructure community.

NIST could continue to be mindful of other resources and guidance being produced. There are many duplicative efforts in the supply chain space. NIST coordinating with other groups to make sure appropriate alignments exist to the CSF and the materials helps the CSF to continue as the foundation.

Consider recommending protocols for emergency management when supply chain exploits occur, including reporting requirements for impacted vendors. Consider a central clearinghouse for vendor reporting suspicious activity. Otherwise, there is a delay in awareness of suspicious activity and subsequent investigation and remediation.

Cybersecurity Supply Chain Risk Management

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.*

In general, consider guidelines for vendors and tools targeting reporting and remediation for supply chain risk.

HARDWARE:
Having a certification lab (as used for safety and energy efficiency standards) for equipment would be helpful. Most companies do not have the resources to reverse engineer to determine if there is a risk in the electronics under question. For example, many energy companies use common suppliers for mission critical systems; having a required or common testing method to alleviate concerns would be beneficial.

SOFTWARE:
Standards or tools for software assurance would be helpful. A standard for supply chain to provide their specific internet connectivity requirements for their products (to enable effective firewall filtering) and for their products to be designed to use least privilege concept.

NIST could also coordinate with the appropriate agencies to ensure that lessons learned following cyber-events are disseminated and aid in maturing supply chain practices across industry.

Cybersecurity Supply Chain Risk Management

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 achieving greater assurance throughout the software supply chain, including for open-source software?*

This is a particularly challenging topic to address, and guidance from NIST on how to properly review it for security and/or secure open-source software would be beneficial. NIST software and supply chain guidance does not adequately address open-source software. NIST does offer guidance that can be applied and tailored to SSO, but no explicit guidance. Additionally, keeping SBOMs current from vendors and requiring SBOMs to be provided to the private sector, would support this effort.

Note that smaller companies may not be aware of other supply chain guidance and are focused on supply chain mandates like NERC CIP 13.

Cybersecurity 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.*

The NIST CSF should apply as much to the supplier as to the consumer. NIST could potentially expand the Supply Chain Risk Management category with sub-categories along with informative references. Creation of contract terms beyond the *Identify* Function would also be helpful. The challenge would be ‘what are the controls needed for just supply chain risk management’.

The technical controls are the NIST 800 series. Consider defining the supply chain risk management and vulnerability management capability and requirements, developing recommendations for coordinating bodies with oversight, and defining mandatory requirements for Supply Chain assessment and reporting.

For smaller companies, integration and simplification is valuable along with quick start “tool kits.” Many smaller organizations are resource-constrained and will move on to quicker/less resource intensive frameworks.