https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

This document has a comment period that ends on 04/25/2022.

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.	
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?	Within the ATO Cybersecurity Group, we have used the CSF to communicate with our management and budgetary personnel. The CSF provides a different way to show the vulnerabilities and exposure levels to management and provide justifications for our budget requests. The CSF provides a better assessment of risks from an organizational level, rather than system specific. It has assisted leadership with understanding the scope of the organizational risk, when presented as the number of systems with POAMs specific to the NIST 800-53 controls mapped to the CSF subcategories. Within the ATO Cybersecurity Group, the tiers have been replaced with a tailored CMMI maturity levels (1 - Initial and 5 - Optimized) and for subcategories qualitatively assessed, a percentage of the systems without associated POAMs (i.e. 1 - 0% to 20% of systems do not have associated POAMs and 5 - 80% to 100% of systems do not have associated POAMs).
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).	Within the ATO Cybersecurity Group, the tiers are not used. Instead, subcategories are assessed qualitatively (using a tailored CMMI assessment) and quantitatively (using a percentage of systems compliant with the ATO tailored controls, derived from NIST 800-53).
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.	The tiers should be changed to be more applicable to the subcategories. It is a struggle to apply the tiers and explain the management how the subcategory proceeds through the tiers.
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.	Changes to the functions, categories, and subcategories would not have a large impact on our usability or backward compatibility. Our group rates the subcategories and levels up to the functions for higher level briefing, when applicable.
6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.	Mapping the subcategories to more specific NIST 800-53 controls, such as AC-01.a, rather than AC-01, would be useful, as our group currently tracks POAMs at the lower level controls. Also, mapping to the OMB 8 categories to the subcategories would be useful, as we mapped and used the CSF subcategories for justification of budget requests.
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: - 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.	Mapping the subcategories to more specific NIST 800-53 controls, such as AC-01.a, rather than AC-01, would be useful, as our group currently tracks POAMs at the lower level controls. Also, mapping the subcategories to steps within the RMF would help (such as ID.AM-5 mapping to Categorize in RMF - ensuring all systems have received a FIPS 199 categorization rating), where applicable. For the subcategories related to training or defining cybersecurity roles and responsibilities, please identify the resources that provide the guidance to meet the intent of the subcategories (i.e. ID.AM-6 and ID.BE-1). Since many system owners and leadership understand the RMF process to obtain yearly authorizations, the CSF appears to be a separate entity, rather than a higher level framework that can show how effective our organization is in applying the RMF and other NIST guidance.
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?	The OMB has 8 categories that our organization has to request, track and report against our budget. Our organization uses the CSF to help justify the budget requests. It would be helpful to map the subcategories to the 8 OMB categories to help with mapping the budget between CSF and OMB. The 8 OMB categories are: 1. Zero Trust / Zero Trust Architecture 2. Endpoint Detection and Response (EDR) 3. Logging 4. Identity, Credential, and Access Management (ICAM) 5. Encryption 6. Security Licensing 7. Incident Response Program Enhancement 8. Modification of Contracts

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?	
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.	Linking NIST 800-161, Cybersecurity Supply Chain Risk Management to NIST 800-53 controls and the supply chain subcategories in the CSF.
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?	NIST breaks out Tier 1,2,3 within an organization. It acknowledges sub-contractor tiering within organizational vendors, but it does not clearly breakout and address contractual requirements that should be assessed by the program on the vendor at all vendor levels. This clear breakout would be useful.
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.	
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?	A continued and deeper dive into identifying and associating threat vectors would be useful i.e., Mitre att&ck and Mitre d3fend into CSF.
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.	A recognition of both the boundaries and intersections of traditional widget SCRM and C-SCRM practices would also be very useful.