NIST Seeks Input to Update Cybersecurity Framework & Supply Chain Risk Management Resources

Comment Number	NIST Suggested Topic #	NIST Suggested Topic	Risk Branch (Team Name)	Team Member	Critical, Substantive Comment	Comment
1	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.	HVA	M. Creary	Substantive	The organization of the CSF into five functions enables agencies/organizations to group cybersecurity outcomes closely tied to programmatic needs and particular activities. This in turn allows for the management of risk tying back to a common framework and streamlined communications of risks.
2			HVA	A. Kamara	Critical	With the on-going efforts by organizations to migrate from on-prem to the cloud, NIST should consider how organizations will actively manage risks if they leverage cloud services, and define how organizations will deal with shared responsibility specifically for Organizations with limited resources.
3	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?	HVA	M. Creary	Substantive	The organization of the CSF into five functions enables agencies/organizations to group cybersecurity outcomes closely tied to programmatic needs and particular activities. This in turn allows for the management of risk tying back to a common framework and streamlined communications of risks.
			HVA	A. Kamara	Substantive	For risk purposes, standardization is crucial. Organizations should ensure that potential vendors follow the CSF model to ensure security. There should be transparency between organizations and entities and measure implemented to show that potential vendors meet Tier 4-Adaptive maturity level. Alternatively, a vendor should provide a security certification from industry leading frameworks such as ISO 27001 for additional assurance.
4			Risk Branch	C. Livingston	Substantive	It is important to ensure the cybersecurity language used regarding the management of risk is understood outside the cybersecurity practioner audience, with particular emphasis to non cybersecurity stakeholders such as supply chain partners, customers, insurers etc.
5	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).	HVA	M. Creary	Substantive	Challenges that may prevent an org from using the CSF framework more easily or extensively include organizations that are not conducting aggregation, normalization, and prioritization of risks in a consistent manner.
6			HVA	M. Sawyer	Substantive	One of the challenges will be proper interpretation of the framework. Due to the complexity of the Framework, the lack of understanding of how to implement it may exist, as it is generic and not specific to each organization.
7			405(d)	N. Douglas	Substantive	One of the challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively is the complexity of the requirements. An approach that could be considered would be to reach for sector specific guidance such as the healthcare sector that may not have the adequate resources to implement the requirement. Also, interpreting the requirements can be a little difficult for a private organizations medical IT staff that may not understand what the terminology means. If there were a section that could act as a crosswalk per sector that would translate the processes, it would assist with the complexity or make it easier to implement. Additionally, the NIST framework could be more helpful for the HPH sector by providing additional guidance on the risks associated with legacy medical devices and the risk to patient safety due to the supply chain- cybersecurity needs that could cause a delay in new application development.
8			HVA	A. Kamara	Substantive	Bandwidth constraints may be a challenge, however, this may be mitigated if agencies/organizations develop and apply standards of procedures for implementation; this can ensure the enterprise has adapted the framework.
9	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.	HVA	M. Creary	Substantive	A mapping of the three Risk Management tiers (implementation/operations level; business/process level, and senior executive level) and inclusion of NISTIR 8286 series references to the CSF Informative References would be helpful.
10			HVA	S. Webster	Substantive	Incorporate the correlation of the CSF to the cybersecurity needs/requirements of small businesses as well as the adoption of the CSF into the practices and standards of international enterprise systems allowing for better global collaboration.
11			HVA	A. Kamara	Substantive	The current Tier level is sufficient. However, it would be beneficial to include a Tier 5, called Managed/Sustained. This tier can indicate that not only has an organization adapted the CSF, but that the organization has countermeasures to ensure that that risks are managed.
12	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.	HVA	M. Creary	Substantive	I believe the current structure makes it easy to use. It is clear and succinct. Anything over 4 columns may become overwhelming.
13			HVA	M. Sawyer	Substantive	Depending on the type of impact to usability, many organizations may see the need to use the framework. Backward compatibility could also have a favorable impact on organizations in terms of adoption.

14	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).	HVA	M. Creary	Substantive	The CSF roughly encompasses NISTIR 8286 series in categories and subcategories (i.e. ID. RA, ID. RM; ID. RS, etc.). However, suggest inclusion of reporting, monitoring, and risk treatment be included with the RM function.
15	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?	HVA	M. Creary	Substantive	It would be useful to do a cross-mapping to cyber-related executive orders such as EO 14028 and related memoranda.
16	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?	HVA	M. Creary	Substantive	Service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of organizations, consistent with organizational requirements (see E.O. 14028 subsection 2 (c)(I)) Information and communications technology (ICT) service providers report back to organization when a cyber incident is discovered involving a software product or service provided to the organizations see E.O. 14028 subsection 2 (f)(I)
17			405(d)	N. Douglas	Critical	An approach that NIST could consider to achieving greater assurance throughout the software supply chain to update the cybersecurity framework pertains to open-source software and providing additional guidance around properly securing them from known exploits. This would provide support to smaller private organizations that may not have the funding to purchase software licenses and due to the supply chain delays generally turn to open-source tools for their cybersecurity needs across the HPH sector.
18			HVA	S. Webster	Substantive	NIST may build on its current work on supply chain security by recommending cyber hygiene practices for vendors and suppliers which allows companies to evaluate their cybersecurity in conjunction with their business partners and customers.
19	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.	HVA	S. Webster	Substantive	Recommend implementing a standard approach to supplier risk in order to modernize C-SCRM processes. Doing so will give suppliers "standard security requirements" and incentivize them to make compliance a priority as well as making their enhanced security awareness and posture more attractive to their clients.
20	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.	GRC	J. Chua	Substantive	NIST may consider developing a C-SCRM Framework, similar to the Privacy RMF, if the NICCS stakeholders identify that a separate framework is needed. If it makes sense to incorporate C-SCRM into the CSF, that would create a more robust and holistic risk management framework to inform and guide an organizations risk management strategy, including integration of the NISTIR 8286 concepts.

The following comment categories have been established:

- **Administrative** comments correct what appear to be inconsistencies between sections, and typographical or grammatical errors.
- **Substantive** comments are provided because sections in the publication appear to be or are incorrect, incomplete, or confusing.
- **Critical** comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.