RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Submitted by: Easy Dynamics on 4/22/2022

General Comments:

Easy Dynamics is pleased to submit comments in response to the Request for Information (RFI) to gather information about evaluating and improving cybersecurity resources for the CSF. We have used the CSF to conduct a risk assessment and develop a CSF profile for the Payroll Industry. You will find that most of our comments reflect that background. We also recognize that it's likely we have used these materials in somewhat non-traditional ways, including rearranging controls across the five categories for our own purposes, tailoring language and process steps to be industry-appropriate, etc. We do not wish to imply that the CSF should be reorganized to fit our approach; rather, we have appreciated the flexibility to use and combine parts of different toolsets to fit our unique needs. Thank you for the opportunity to submit comments and we look forward to a continued partnership with NIST.

RFI Specific Comments:

Question (1-14)	Comments
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.	We found the CSF very helpful in organizing risk via the five functions. We used it in concert with the RMF to conduct a risk assessment and identify controls tailored to our industry. Since this exercise was conducted on behalf of an industry, rather than within a single organization, we have limited insight into how the CSF is being used to actively manage risk at any one entity; but the framework was helpful in creating a profile to provide guidance and best practices and to be leveraged by industry professionals as a tool in reviewing their cybersecurity posture against the CSF. We have received indications that the profile is in use across industry members of mostly small and medium-size businesses.
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?	We have found an increased comfort level with discussing cybersecurity terms, concepts, and controls among industry membership since publishing the CSF profile. Most of our audience is non-technical and using the CSF as an introductory tool, that is more digestible with references back to the more detailed publications, provided an easier entry point into these conversations. The CSF allowed for better assessment of risk specific to the industry rather than simply selecting the moderate level baseline from 800-53 and going through each control. We opted for a checklist format rather than the formal implementation tiers to match the style of other industry legislation (i.e. FTC Safeguards Rule) but the concept is the same and helps provide a roadmap for ongoing risk management. Since our industry is concerned with fraud and identity theft, metrics may include: reduction in fraud or attempted fraud; number of suspicious or confirmed incidents (either % increase/decrease or as a result of monitoring and detection); personnel comfort level or awareness of cybersecurity topics.

Question (1-14)	Comments
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).	We believe that the length/volume of the CSF materials may be a perceived barrier for non-technical users who are not familiar with the framework; however once users became nominally familiar with the CSF toolset, they reported increased comfort levels quickly. Challenges to adoption or effective use include the lack of legal guidance and regulation for the industry around cybersecurity, data security, and privacy requirements, resulting in mixed approaches and attitudes toward implementation. Small and medium-size organizations in particular cite less incentive to implement risk management due to the perceived belief that they are not a target. In addition, smaller organizations may not have the technical staff to set up and manage more complex backend controls and may have trouble finding/ implementing third party solutions. Resources are also an issue, especially when management views risk probability as low.
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.	Potential modifications to the content may include: • **Protect** - many smaller organizations use federated logins e.g. through Facebook; consider emphasizing controls for this area. • **Protect** - cyber insurance can be an important protection to mitigate the severity of attack impact; consider emphasizing controls for this area. • **Protect** – since multi-factor authentication is becoming more essential even for lower-risk systems, consider including specific recommendations to use MFA. • **Detect** - payroll industry is very concerned with fraud mitigation. While not traditional cybersecurity per se, we believe fraud is a breach of integrity of sorts; consider emphasizing additional anti-fraud principles such as out of band approvals, identity validation against authoritative sources, flag creation and monitoring, role redundancy, or data validation. • **Identify/Respond** – reporting and communication of incidents is becoming increasingly important; while these are captured in the Respond step, consider emphasizing the creation of a communications/reporting plan as part of ID.GV. Potential modifications to the general framework include: • Adding reference to further NIST publications within the Excel sheet itself. We found a helpful reference page but only discovered it after our work was completed. If not directly in the Excel, perhaps a link could be included in a readme tab.
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.	Limited impact expected to the Payroll profile.

Question (1-14)	Comments
6. Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.	Limited additional comments beyond the details provided.
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.	We used the RMF to guide our risk assessment and the CSF to support the control selection process in creating the profile. The RMF could have pointed more clearly to the CSF for this purpose, although we may not have been using the two in the correct way together. Perhaps a flowchart of "which resources do I use" at each step of the RMF would be helpful (apologies if this exists already). We benefitted from using the RMF because it gave clear guidance on how to categorize systems and identify and prioritize risks. We used the Privacy Framework to guide additional risk identification and control selection for inclusion in the profile. We used SP 800-53-5 for additional control selection and deepening our understanding of control families. We also perceived some discrepancies in terminology across resources, for example SP 800-61 has an incident response lifecycle (Section 3.1) that could be better aligned to the five stages of CSF. Also, this is across agency boundaries, but CISA's incident response playbooks use this slightly different terminology as well. We found it helpful to have the CSF mapped to SP 800-53-5 as well as the Privacy Framework.
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?	We drew from a variety of non-NIST resources to create the profile, including FTC Safeguards Rule data protection requirements; CISA incident response guidance; and risk identification techniques like STRIDE. We did not encounter any specific conflicts except for terminology discrepancies such as mentioned in comment #7.

Question (1-14)	Comments
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?	One aspect that we had to "DIY" was the inclusion of sector-specific regulations such as the FTC Safeguards. International legislation like GDPR or other EU regulations would have to be similarly analyzed by CSF users and their laws incorporated on their own. It may be helpful to incorporate these into informative references or to create a set of overlays that pull out the requirements from these documents and assign them to the five stages framework, so that users who are beholden to these regulations can simplify their compliance. However, we can also understand the view that sector-specific regulations belong in industry profiles and are not the purview of NIST.
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.	See comment above.
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?	No comments for this area.

Question (1-14)	Comments
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.	No comments for this area.
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?	No comments for this area.
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.	No comments for this area.