SUBMITTED ELECTRONICALLY VIA REGULATIONS.GOV
April 25, 2022

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

Ms. Katherine MacFarland
National Institute of Standards & Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

To Whom It May Concern:

UL appreciates the opportunity to comment on the National Institute of Standards and Technology's (NIST) Notice and Request for Information on The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management. UL supports NIST's effort to seek private sector input to improve the government's cybersecurity resources, including the Framework for Improving Critical Infrastructure Cybersecurity.

Since its inception in 1894, UL serves a mission of promoting safe living and working environments for people everywhere and fulfills a promise of facilitating the flow of goods across borders. UL's work engenders trust in pioneering technologies, from electricity to the internet. Our 1000s of scientists and engineers safeguard and facilitate innovation, advance safety breakthroughs and identify and address risks associated with every wave of innovation. We are constantly seeking new ways to identify hazards and help manufacturers, governments, and consumers mitigate them.

UL enables trust and vital end-to-end security designed for our interconnected world. We possess a unique expertise in developing security frameworks, structuring security programs for IT and interconnected ecosystems through to security and identification / authentication, evaluations and verification. Our expertise and independence enable businesses to innovate without compromising on security while engendering customer trust resulting in greater market access.

Please find below UL's detailed responses to a subset of the questions posed in the Request for Information. As NIST moves forward with its efforts to update and improve the nation's cybersecurity resources, UL is eager to share our expertise with NIST. If you have any questions regarding this submission or would like to discuss UL's recommendations further, please do not hesitate to contact Dean Zwarts at [redacted]. Thank you for your attention to these comments.

Respectfully,

Derek Greenauer
Director, Global Government Affairs

UL LLC
1850 M St. N.W., Suite 1000, Washington, DC 20036-5833 USA
T: 202.296.1435 / F: 202.872.1576 / W: UL.com

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.***

   The NIST CSF aids organizations in establishing cybersecurity efforts by providing direction on where to start (Identify) to meet the cybersecurity needs and how to define processes to Recover from security incidents. The value that the CSF offers organizations is flexible process (approach) for companies to employ to manage their own cybersecurity risks. The framework helps an organization to implement an information security management system like that of ISO 27001. The main categories of the CSF that are focused on managing risks are Risk Management Strategy (ID.RM), Risk Assessment (ID.RA), and Supply Chain Risk Management (ID.SC) for which an organization may need to rely on a risk management framework such as ISO27005, ISO31000 and NIST SP 800-37.

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?***

   Comment 1 **–** *"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?"*

   The goal of the NIST CSF is to help organizations better manage and reduce cybersecurity risk. NIST CSF covers risk management in the categories of Risk Assessment (ID.RA), Risk Management Strategy (ID.RM) and Supply Chain Risk Management (ID.SC). The subcategories under each provides high-level statements on what should be done, such as "risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders". For an organization to implement a framework to manage risks, it will need to refer to additional standards such as ISO 27005 or NIST SP 800-37 because these frameworks provide more detailed / in-depth set of processes which need to be implemented in the organization to manage risks. These standards cover the full life cycle of risk management such as defining the basic criteria of managing the risks and how to monitor, review and improve the overall process of risk management itself which the NIST CSF does not cover in detail (as Informative References section of these subcategories refer to other standards and frameworks such as COBIT, ISO 27001 or NIST SP 800-53).

   Comment 2 **–** *"What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?"*

   A simpler approach to define metrices for improvement would be to determine how many categories or subcategories have achieved higher tiers for the current profile or target profile of the organization.

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).***

When an organization needs to implement an information security framework or a standard one of the most important question for which it is looking for an answer is “What is the Scope?”. Usually the scope is People, Process, Technology and Locations (for physical security) where the Categories/Subcategories or controls must be implemented. While implementing NIST CSF, an organization also needs to identify the current profile and the target profile (i.e., to select which controls should be applied). An organization evaluates the threats and risks that it is facing. While the framework’s goal is to manage cyber security risks, it does not highlight which threats are being covered or mitigated by implementing each Category/Subcategory or the need to implement them. The ISO/IEC 27005:2018 provides examples of threats and vulnerabilities in Annex C and Annex D respectively and referring these threats and vulnerabilities to Category or Subcategory can better help risk practitioners to implement and manage risks.

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.***

Comment 1

The natural flow of risk management is first, to define the risk management approach and evaluation criteria and then identify assets and threats related to those assets (refer section 7.2 and 8.2 of ISO 27005). In the NIST CSF, the Category Risk Management Strategy (ID.RM) comes after Risk Assessment (ID.RA). Similarly, internal, and external threats should be identified first before identifying asset vulnerabilities. However, in the framework “*ID.RA-1: Asset vulnerabilities are identified and documented*” comes before “*ID.RA-3: Threats, both internal and external, are identified and documented*”. This may lead to confusion among the risk practitioners while implementing the CSF when an entity is already using ISO 27005 which is one of the most used risk management techniques.

Comment 2

Recent trends in the threat landscape suggests that ransomware and phishing attacks (social engineering attacks) are at new heights. Hence, we suggest that the NIST CSF should include sub-categories for Awareness and Training (PR.AT) on protection against ransomware and phishing attacks, implementing phishing campaigns to identify employees, sub-contractors, or vendors vulnerable to such attacks, implementing measures to repel and recover from such attacks etc. Refer (https://www.cisa.gov/uscert/ncas/alerts/aa22-040a)

Comment 3

Due to the Covid-19 pandemic, mindsets regarding working from office have changed and employees can now work from anywhere in the world if they have an internet connection. They may use equipment (laptops/desktops, mobile devices etc.) provided by their organization or can use their personal equipment. If such a device is misplaced, lost, or stolen, a person with malicious intent may be able to gain access to critical information and systems of the organization. Hence, organizations need more control on such equipment more than ever. Organizations should have a BYOD and teleworking policies and procedures in place to manage such scenarios according to their business needs. Such controls should be added as Subcategories under the Function Identify

and Protect. Organizations should also be required to periodically review logs generated by this equipment to identify and respond to any security event.

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.***

An organization, to keep itself secure, must constantly keep up with the latest trends in cybersecurity threats and accordingly implement necessary controls to mitigate them to improve its overall security posture. For most organizations it is a continuous process and hence if the Functions, Categories, Subcategories, etc. is modified or changed then organizations can also pick up with the new changes in the framework too. Until and unless material changes are made to the NIST CSF Functions, Categories, Subcategories etc., it should not impact the usability and backward compatibility of the NIST Cybersecurity Framework, but that would depend on the nature of the change.

6. ***Additional ways in which NIST could improve the Cybersecurity Framework or make it more useful. Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources.***

Comment 1

The subcategory "PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities" suggests that systems should be configured in a manner such that only necessary services are running. The informative reference given for this subcategory from ISO/IEC 27001:2013 is A.9.1.2. The intent of A.9.1.2 is that users should be provided with access to network and network services only after specific authorization. Hence, the informative reference for PR.PT-3: should be updated to more relevant controls from latest version of ISO/IEC 27001

Comment 2

UL recommends merging the following categories/ into one that is focused on Roles & Responsibilities of the different parties (suppliers, customers, partners, etc.). Combining them would be more convenient and sensible for cyber security practitioners during implementation as there is overlap between the two.

- Asset Management (ID.AM):
  - ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
- Awareness and Training (PR.AT):
  - PR.AT-2: Privileged users understand their roles and responsibilities
  - PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
  - PR.AT-4: Senior executives understand their roles and responsibilities
  - PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

Comment 3

NIST may want to include a new framework core – Improve – in the NIST CSF to monitor and measure the overall cybersecurity efforts of an organization and organizations should be at liberty to choose the parameters or criteria (KRIs, KCIs, KPIs according to their business needs and

strategies to measure and monitor) for each of the core categories or subcategories that are deemed fit by the organization.

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.***

   UL suggests that because there are number of risk management standards and frameworks available and to which the organizations are already complying, NIST CSF should provide the option for such organizations to automatically consider themselves compliant to the Categories - Risk Management Strategy (ID.RM) and Risk Assessment (ID.RA). Essentially, these Categories refer to the NIST SP 800-37 or ISO 27001. NIST CSF should include and maintain a list of accepted standards or frameworks that align with the CSF.

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?***

   Please refer to Comment 1 of Q4.

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?***

   There are several information security standards which focus on security of a specific type of data (and supporting infrastructure) such as Account Data in PCI DSS standard, PINs and keys in PCI PIN standard, PIIs/Health data in HIPPA/HITRUST CSF and so on and so forth. While some of these standards (such as PCI DSS, ISO 27001) overlap to a higher degree with NIST CSF Categories and Subcategories, other standards such as PCI PIN, PCI SSS or PCI SLC, Card Production Logical and Physical Security do not. Such standards with a narrow or specific focus area may not be interoperable with NIST CSF. To ensure increased international use of the CSF, NIST may want to –

a. Provide guidance on how using a specific product or service, an organization can meet the NIST CSF requirements. (Although it is of the interest to organizations providing products or services to prepare documentation which shows mapping between NIST CSF Categories and Subcategories to the features or usage of products or services, NIST may want to encourage such organizations to publish such articles). This would provide guidance or direction to organizations who are using those products or services to meet the CSF requirements.
b. Add more information security standards in Informative References.
c. Highlight unique usability of the CSF through publicly available case studies.

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*.**

    In addition to the standards and publications already listed in the question and in the framework itself, NIST CSF Informative References should include UL2900, ISO 27005, ISO 31000, PCI DSS, PCI SSS, PCI SLC and PCI PIN standards.

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?***

    Today, hackers are compromising update servers and then when the updates are pushed to or downloaded by the clients, they become compromised. The SolarWinds hack is one recent example. UL believes this practice is also a great challenge related to the cybersecurity aspects of supply chain risk management because organizations are trusting the update servers (which are not located at the organization's end) for patches, updates, or hotfixes etc. for fixing the issues rather than compromising them. If such fixes are considered as precious (a commodity), then production (creation) of patches and its distribution also falls under the definition of supply chain.

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 specific comment.

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 specific comment.

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 specific comment.