HO·CHUNK
INCORPORATED

1 Mission Drive • Box 390
Winnebago, NE 68071

800.439.7008
402.878.2809

www.hochunkinc.com

VIA Federal e-Rulemaking Portal – Regulations.Gov

April 25, 2022

Katherine MacFarland
Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
(301) 975-2762

Dear Ms. MacFarland:

On behalf of Ho-Chunk Inc. (Ho-Chunk), I am pleased to submit this response to the Request for Information (RFI) published in the Federal Register (FR) on February 22, 2022. The RFI requested information that would support the identification and prioritization of supply chain-related cybersecurity needs across sectors.

Background:

Ho-Chunk, Inc. is a parent company to tribally owned government contractor subsidiaries providing economic development to the Winnebago Tribe of Nebraska, and we understand why cybersecurity protection is so important. The work of Ho-Chunk, Inc. and its subsidiaries has been consistently recognized for excellence in operations and honored for its work in federal government contracting. As a parent company of small businesses supporting critical missions of various U.S. government customers, our goal is to provide quality services within our capabilities in federal contracting. Ho-Chunk, Inc. understands that protecting the data received from our government customers is critical and that there are foreign adversaries who pose a risk to that data on a daily basis. We hope that our viewpoint as a small, disadvantaged business will prove valuable to the National Institute of Standards and Technology (NIST) in evaluating and improving its cybersecurity resources.

Recommendations and Comments:

The NIST Cybersecurity Framework was last updated in April 2018. NIST indicated in the February FR notice a non-exhaustive list of possible topics that might be addressed in any industry comments. We submit the following recommendations or comments from our viewpoint as a parent company of several small companies who must be compliant to the NIST Cybersecurity Framework in our government contracts.

TOPIC: 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.

Response: The overall cybersecurity framework as defined in NIST 800-171/171a was very helpful in understanding "what" needs to be done to have a good cybersecurity platform. The broader cybersecurity frameworks span multiple related standards and is confusing in terms of knowing how to relate. In addition, more directions on the "how" to implement controls would be helpful.

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?

Response: The details in NIST 800-171 do provide a good framework for communicating the cybersecurity requirements across the internal organization and external partners. It also provides criteria that can be used to assess risks. When considering NIST 800-171, the Assessment Guides and SPRS scoring are the key metrics.

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).

Response: The fact that there are multiple control families (e.g. 800-53, 800-171, 800-161, DFARS, etc.) in the framework with no good mapping between control requirements from each of the families makes it confusing. Understanding and implementing all the applicable controls is complex, resource intensive, and expensive to build and operate.

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.

Response: The first thing that is needed is a comprehensive, relatively easy to understand road map across all Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines. Ideally it would be in an automated format that would allow organizations to search for a specific control and then see all related topics across all frameworks. Currently all those things are independent silo's and require implementing organizations to search across all the silo's and determine what is required. Unfortunately, that makes it easy to inadvertently miss critical control information.

Current frameworks are heavily oriented to application development in a single on-premises datacenter. There is little acknowledgement or guidance on use of cloud solutions integrated in the frameworks

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.

Response: Depending on the degree of change, the potential exists to invalidate the investments made in achieving compliance with a prior framework.

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

Response: There could be more definition that would relate to other frameworks.

TOPIC: 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.

Response: There is no good resource to make the correlations between the various areas.

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?

Response: There is benefit to more mapping control details to the framework.

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?

Response: We suggest closer integration with ISO 27001 and 27002 and incorporation of the privacy framework into the NIST framework from GDPR and PIPEDA.

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.

Response: We believe the following references should be considered for inclusion within the NIST. The Health Insurance Portability and Accountability Act (HIPAA) documents; Purchased Care Detail Information System (PCDIS), North American Electric Reliability Corporation – Critical Infrastructure Protection Standards (NERC-CIP), Criminal Justice Information Services (CJIS), and American's Water Infrastructure Act (AWIA).

TOPIC: 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?

Response: Using the appropriate controls based on what it was built to do and how it is used. Smaller vendors and suppliers don't have the capability to do that. The skillset and acumen to do that is concentrated to larger entities or entities where supply chain security is essential to ongoing business. There is a lack of awareness of security requirements in the development of control software that is created and installed by the Original Equipment Manufacturer (OEM).

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.

Response: We have no comment or recommendation on this topic.

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?

Response: NIST has a huge blind spot for cloud services. Cloud services should be considered first before any other area mentioned in this question.

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.

Response: Please see our previous response covering cloud services.

C**onclusion:**

Ho-Chunk Inc appreciates the opportunity to comment on this very important Framework. Please do not hesitate to contact us if you would like any further information.

Sincerely,

04/19/2022 | 9:21 AM PDT

DocuSigned by:

Annette Hamilton

CFFF9E84227C4C8...

/s/ Annette Hamilton

Annette Hamilton

COO - Ho-Chunk, Inc.