PUBLIC SUBMISSION

As of: 4/25/22 12:51 PM
Received: April 24, 2022
Status: Pending_Post
Tracking No. l2d-jqmw-8662
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0035
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: SideChannel, Inc.

General Comment

Background: We founded SideChannel with the belief that small and mid-sized organizations deserved the expertise of an experienced CISO just as much as a larger enterprise, but at a reasonable cost. Today, we’re helping organizations all over the world improve their cybersecurity and move their mission forward. Merging proven experience with an innovative virtual model, we act as a natural extension of your team — taking the time to identify the organization’s unique security gaps and offering the services and guidance required, when they are needed.

Our founder and CEO, Brian Haugli, first implemented the NIST CSF while leading the information assurance program for US Army ITA at Pentagon from 2011-2015, then was one of the earliest adaptors and fully implemented NIST CSF at a Fortune 500 Financial Services company in 2015. Brian has been recognized as an expert on the Framework, spoken widely on it’s practical use for companies and is the contributing author on a recently published book from Wiley titled, “Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework”.

Contact Information:
SideChannel, Inc.
146 Main St, Suite 405
Worcester, MA 01608
https://www.sidechannel.com
info@sidechannel.com

See attached file(s)

Attachments

SideChannel

NIST Cybersecurity RFI Submission - SideChannel, Inc.

Background: We founded SideChannel with the belief that small and mid-sized organizations deserved the expertise of an experienced CISO just as much as a larger enterprise, but at a reasonable cost. Today, we're helping organizations all over the world improve their cybersecurity and move their mission forward. Merging proven experience with an innovative virtual model, we act as a natural extension of your team — taking the time to identify the organization's unique security gaps and offering the services and guidance required, when they are needed.

Our founder and CEO, Brian Haugli, first implemented the NIST CSF while leading the information assurance program for US Army ITA at Pentagon from 2011-2015, then was one of the earliest adaptors and fully implemented NIST CSF at a Fortune 500 Financial Services company in 2015. Brian has been recognized as an expert on the Framework, spoken widely on it's practical use for companies and is the contributing author on a recently published book from Wiley titled, "Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework".[1]

Responses from SideChannel are in RED.

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.

Continue the five functions in the Framework as the core. Begin to include the narrative that each can inform the other and the five are cyclical; ie, Recover can lead to betterment of Identify Category controls.

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?

[1] Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework - https://www.wiley.com/en-us/Cybersecurity+Risk+Management%3A+Mastering+the+Fundamentals+Using+the+NIST+Cybersecurity+Framework-p-9781119816287

There seems to be a disconnect and lack of usage of the implementation tiers. A suggestion would be to tie each tier and description to each of the 108 Category controls, thus creating a maturity model of 1-4 for each. This is one area that is lacking when organiztions wish to see how well they meet each Category control. The current version presents as a "all or nothing" view.

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).

Two challenges are present; true understanding of what the Framework means and when to use it. While many cybersecurity professionals can surpass these challenges, many non-cybersecurity professionals struggle to understand the fit or application of the Framework.

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.

Recommend adding more robust mapping of controls and other frameworks. Many organizations either wish to or are bound by requirements to meet a variety of frameworks. A more robust cross mapping from NIST would create more authority to how organizations can present when and where they meet each Category control. This would also lead to increased adoption and reduced workloads along with costs.

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.

If the Framework does not radically change their controls, identifiers, or descriptions, we do not foresee any issues with usability and backward compatibility.

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

Further adoption and continued use of Open Security Controls Assessment Language (OSCAL).

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.

No recommendations at this time.

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?

Recommend further cross mapping to the Center for Internet Security (CIS) Controls. These present a tactical and operational set of criteria to meet the more high level risk management style NIST CSF Category controls.

Recommend a more robust mapping to the ISO 27000-series. The ISO framework's adoption is significant and many organizations incur significant costs when pivoting from ISO to NIST (and vice versa). A more authoritative and robust cross mapping will lead to lower costs and higher adoption of the NIST CSF.

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?

No recommendations at this time.

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.

Recommend including reference to the book out from Wiley by contributing author Brian Haugli, “Cybersecurity Risk Management: Mastering the Fundamentals Using the NIST Cybersecurity Framework”.

Filled with clear and easy-to-follow advice, this book offers readers:

- A concise introduction to the principles of cybersecurity risk management and the steps necessary to manage digital risk to systems, assets, data, and capabilities
- A valuable exploration of modern tools that can improve an organization’s network infrastructure protection
- A practical discussion of the challenges involved in detecting and responding to a cyberattack and the importance of continuous security monitoring
- A helpful examination of the recovery from cybersecurity incidents

Contact Information:

SideChannel, Inc.

146 Main St, Suite 405

Worcester, MA 01608

https://www.sidechannel.com

info@sidechannel.com