Summary Analysis - Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop #1 August 17, 2022

National Institute of Standards and Technology (NIST)
Issued September 9, 2022

Introduction

On August 17, 2022, the National Institute of Standards and Technology (NIST) hosted its first public workshop on the update to the NIST Cybersecurity Framework (CSF). NIST is updating the CSF to keep pace with the evolving cybersecurity landscape. The CSF was first published in 2014 after a year-long, collaborative process in which NIST convened industry, academia, and government stakeholders. The CSF is now widely viewed as foundational to securing organizations and technology – not only because it provides a common vocabulary for the cybersecurity community but because of NIST's commitment to the practice of meaningful stakeholder engagement, which yielded broad community buy-in in the early days of the development of the Framework. NIST continues to embrace the stakeholder-driven process as NIST moves to CSF 2.0.

This workshop was one way NIST sought input from stakeholders about the current use of the Framework, as well as how the Framework can evolve to meet today's cybersecurity challenges. The event built on stakeholder input received in response to the NIST Cybersecurity Request for Information, "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management", issued in February 2022.

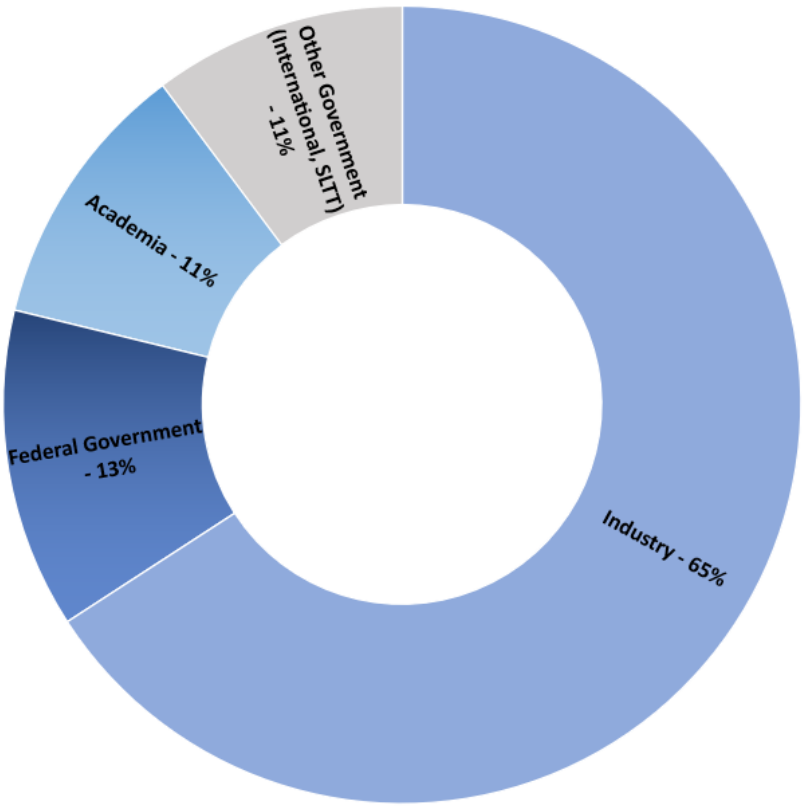
This paper provides a short summary of the workshop. Full recordings of each panel can be found on the workshop event page. The workshop was held virtually, with a combination of expert panels and attendee input through dedicated Slack channels and video webinar Q&A.

Overall, the workshop provided NIST and stakeholders opportunities to:

- Share and learn about organizations' use of the CSF and suggestions for improvements
- Review comments received in response to the recent NIST Cybersecurity Request for Information (RFI)
- Discuss themes identified in the RFI analysis (with a focus on international, governance, measurement, and supply chain topics)
- Learn about – and inform – NIST's next steps for the CSF (and how to get involved)

Participation

Participants were active and engaged through Slack channels and interactive Q&A throughout the two-day event, providing inputs, suggestions and asking questions of panelists and each other. More than 3,900 attendees joined the workshop from 100 countries. Just over 7,200 registered for the workshop and 2,095 joined the dedicated Slack channels for the event. The countries with the highest number of attendees (beside the United States) were: Canada (181), India (89), United Kingdom (89), Brazil (34), Germany (31), Mexico (31), Colombia (20), Singapore (19), Italy (16).



Estimated Breakdown by Organization Type with Approximate Percentage (Registered)

Summary of Workshop Panels

The workshop panels were chosen based on some of the themes identified in the RFI summary analysis, considering commonalities in the RFI responses.

Workshop Panel	RFI Summary Analysis Theme
Panel 1: NIST Discussion of CSF 2.0	All RFI Themes.
Panel 2: Lessons Learned from Development and Use of CSF Profiles	**Theme 3:** Offer more guidance for implementing the CSF **Subtheme 3.1:** Offer more guidance on CSF implementation **Subtheme 3.2:** Provide specific guidance on developing CSF profiles
Panel 3: International Use and Alignment in the CSF	**Theme 2:** Align the CSF with existing efforts by NIST and others. **Subtheme 2.6:** Increase international collaboration and engagement, including alignment with the International Organization for Standardization (ISO) 27000 series.
Panel 4: Consideration of Governance in the CSF	**Theme 2:** Align the CSF with existing efforts by NIST and others. **Subtheme 2.3:** Address the important role of governance in cybersecurity risk management, although there are several different approaches for doing so.

Panel 5: CSF Measurement and Assessment	**Theme 5:** Emphasize the importance of measurement, metrics, and evaluation in using the CSF. **Subtheme 5.1:** Consider and highlight how the CSF is used as an assessment tool, including consider additional guidance on assessment (for self, suppliers, products, and services). **Subtheme 5.2:** Provide a means to measure CSF implementation. **Subtheme 5.3:** Expand on (or, in contrast, remove) Tiers and include (or do not include) guidance on maturity models.
Panel 6: Consideration of Supply Chain Cybersecurity in the CSF	**Theme 6:** Consider cybersecurity risks in supply chains in the CSF. **Subtheme 6.1:** Address supply chain risks, either in the CSF or separately. **Subtheme 4.2:** Consider the importance of software security, either as part of the CSF or in conjunction with the CSF.

Opening Remarks from the NIST Director and National Cyber Director

The Honorable Laurie E. Locascio, Under Secretary of Commerce for Standards and Technology and Director, NIST
The Honorable Chris Inglis, National Cyber Director, Executive Office of the President
Cherilyn Pascoe, Senior Technology Policy Advisor, CSF Program Lead, NIST

NIST Director Locascio and National Cyber Director Inglis provided opening remarks, stressing the value of the CSF in improving cybersecurity risk management, and providing their support for the CSF 2.0 update process.

Panel 1: NIST Discussion of CSF 2.0

Moderator: James Lewis, Senior Vice President and Director, Strategic Technologies Program, Center for Strategic and International Studies (CSIS)
Panelists: Jon Boyens, Deputy Chief, Computer Security Division, NIST; Amy Mahn, International Policy Specialist, NIST; Cherilyn Pascoe, Senior Technology Policy Advisor, NIST; Adam Sedgewick, Senior Technology Policy Advisor, NIST

In this first panel, NIST staff discussed the drivers to update the Framework now and the update process. They explained how panels for the day were selected based on the NIST RFI analysis themes on CSF guidance, international engagement/alignment, and additional considerations of governance, supply chain and measurement. Staff emphasized how the CSF 2.0 could be leveraged to increase usage of the CSF, including through increased awareness of existing resources (while also filling gaps in implementation guidance for small and medium sized organizations). They noted the importance of updating the Framework to keep pace with changes in standards and technology. This will require changes to the CSF along with additional mappings to new standards. Staff reinforced the need to keep the CSF technology neutral, while also recognizing the changing landscape due to cloud computing, an increasingly hybrid workforce, and the continual growth of the internet of things. Staff emphasized the importance of international engagement and alignment for the update and outlined NIST's related international and standards development efforts. Finally, as the cybersecurity policy landscape

changes, they noted the importance of engaging government regulators and increasing alignment between the CSF and future regulatory objectives.

Panel 2: Lessons Learned from Development and Use of CSF Profiles

Moderator: Josephine Long, U.S. Coast Guard (Ret.)
Panelists: Rudy Brioche, Vice President and Counsel, Global Public Policy, Comcast; Deborah J. Eng, Executive Director, Technology and Cybersecurity Policy and Partnerships, JPMorgan Chase & Co.; Gema Howell, Lead, Election and Mobile Device Security, NIST; Keith Stouffer, Group Leader of the Networked Control Systems Group, NIST

The second panel discussed how the CSF can be tailored to organizations of various sectors and sizes by showcasing a few examples of sector-specific profiles. Using the CSF, every organization can develop their own profile to tailor the CSF – prioritizing certain categories/subcategories and incorporating sector-specific responsibilities to meet mission and business objectives. Example profiles can be helpful because they do some of the heavy lifting of incorporating sector-specific standards and regulations.

The panel included several experts involved in developing example CSF profiles including:

- NISTIR 8183r1 - Cybersecurity Framework Version 1.1 Manufacturing Profile
- NISTIR 8310 (Draft) - Cybersecurity Framework Election Infrastructure Profile
- The Profile by the Cyber Risk Institute (for the financial sector)
- The Cybersecurity Risk Management and Best Practices Profile by the Communications, Security, Reliability, and Interoperability Council, and
- Cybersecurity Framework Profiles for Maritime Bulk Liquid Transfer, Offshore Operations, Passenger Vessel, and Industry Cybersecurity Processes created collaboratively on behalf of the U.S. Coast Guard

Panelists discussed how the sample profiles were developed and provided examples of how profiles can be tailored to specific sectors, organizations, or components of an organization. They offered views about how usage of the CSF among small- and medium-sized organizations could be increased. Panelists and workshop attendees alike expressed a need for more sample profiles, as well as additional guidance on how to develop profiles and make profiles already on NIST's website more readily accessible.

Panel 3: International Use and Alignment in the CSF

Moderator: Leonard Hause, Bureau of Cyberspace and Digital Policy, U.S. Department of State
Panelists: Kerry-Ann Barrett, Cybersecurity Program Manager, Secretariat of the Inter-American Committee Against Terrorism (CICTE), Secretariat for Multidimensional Security (SMS), Organization of American States; Wen Kwan, Senior Director, ICT Resilience, Innovation, Security and Economic Development Canada, Government of Canada; Laura Lindsay, Cybersecurity Standards Strategist, Microsoft

The third panel highlighted the importance of increasing international adoption of the CSF through engagement internationally and alignment with international standards. This panel focused on ways in

which the CSF principles have been leveraged across the Americas, including in the United States-Mexico-Canada (USMCA) trade agreement, in Canada, and the Organization of American States. It also addressed international aspects of the CSF more broadly, including how countries have leveraged the common language and risk-based approach of the CSF in national policy.

Panelists discussed the importance of engaging in international standards bodies to advance the CSF as well as helping organizations to understand the intersections and gaps between ISO 27000 and the CSF. They also noted the trend of ISO to increasingly leverage the CSF. Several panelists pointed to the success of the CSF in creating a common terminology which enhances the communication among governments. The discussion also covered how some terms vary between countries, such as an emphasis on digital security rather than cybersecurity and how language differences also come into play. Panel members noted barriers for small- and medium-sized organizations in using international standards. They emphasized how the voluntary nature of the CSF has been fruitful and effective in its gaining traction around the globe.

Panelists referenced CSF-related resources and NIST staff shared links through the Slack channel. Some resources that were referenced and shared include:

- NIST International Cybersecurity and Privacy Resources Site, which describes NIST's international engagement, including links to CSF translations and adaptations.
- The Organization of American States (OAS) and Amazon Web Services (AWS) White Paper on the CSF addresses opportunities and advantages of the CSF's cybersecurity risk management approach.
- International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) Technical Reference 27103: Cybersecurity and ISO and IEC standards. This document leverages concepts of the CSF and demonstrates how a cybersecurity framework can utilize current information security standards to achieve a well-controlled approach to cybersecurity management.
- International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) Technical Specification 27110: Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines. This document specifies guidelines for developing a cybersecurity framework—including using concepts that align with the CSF functions.

Panel 4: Consideration of Governance in the CSF

Moderator: Nahla Ivy, Enterprise Risk Management Officer, NIST
Panelists: Julie Chua, Director, Governance, Risk Management, and Compliance Division, U.S. Department of Health and Human Services; Tendai Gomo, Vice President, Head of Cyber Governance and Risk, Capital One; Alicia Rosenbaum, Vice President and Associate General Counsel, Salesforce; Ola Sage, Founder and CEO, CyberRx

The fourth panel examined approaches to governance in addressing cybersecurity risks.

Panel members discussed the challenges in addressing governance given the increasingly interconnected nature of their operating environments and growing dependencies on their supply chain. They stressed: the importance of identifying the roles different people in the organizations play; how the CSF can be used to align cybersecurity risks with business objectives; and how to determine priorities and risk tolerances by engaging senior leadership as well as customers and suppliers in implementing the CSF. Focusing on Enterprise Risk Management, the panel highlighted practices to assist organizations in determining their critical business and mission functions to allow them to better quantify risk reduction.

Several panelists shared insights about how they use the CSF to provide status updates on meeting cybersecurity priorities to their senior leadership, and the Framework's value in carrying out their responsibilities. Discussions among the panelists and Slack channel participants cited some of the unique needs of small and medium businesses and offered ideas on how to get them started in setting up a cybersecurity program – moving away from an all-or-nothing approach and getting started by looking at regulatory requirements and their specific threat landscape.

Panel 5: CSF Measurement and Assessment

Moderator: Lisa Carnahan, Associate Director for IT Standardization, NIST
Panelists: Khalid Hasan, Senior Manager for Information Technology Audits, Office of Inspector General for the Board of Governors of the Federal Reserve Board and the Consumer Financial Protection Bureau; Kelly Hood, Executive Vice President and Cybersecurity Engineer, Optic Cyber Solutions; Alicia Clay Jones, Manager, Policy and Performance, Entergy Services, Inc.

The fifth panel focused on how to enhance cybersecurity measurement and evaluation when using the CSF.

Panelists described how they are using the CSF – both in their organization and in organizations they oversee or guide – and the role of measurement and assessment. The panel shared how they leverage the CSF with other risk management frameworks and maturity models to meet their varying measurement and assessment needs. Measurement and assessment relating to the CSF had different meanings and implementations among the group, depending on their goals. Yet it was clear that each leveraged the CSF as a common means for communicating expectations and current cybersecurity posture with nontechnical stakeholders and for identifying programmatic cybersecurity trends. Each cited the inherent flexibility and risk-based approach of the CSF as valuable in developing innovative and tailored approaches to quantifying and qualifying risk.

Participants in the Slack discussion were especially active in this panel, sharing additional examples of how they are using the CSF for measurement and assessment, additional resources, and opportunities for additional NIST guidance.

Panel 6: Consideration of Supply Chain Cybersecurity in the CSF

Moderator: Nadya Bartol, Managing Director, Boston Consulting Group Platinion
Panelists: David Batz, Managing Director of Cyber and Infrastructure Security, Edison Electric Institute; Paul Eisler, Senior Director, Cybersecurity, USTelecom | The Broadband Association; Mihoko Matsubara, Chief Cybersecurity Strategist, NTT Corporation; Chris van Schijndel, Cybersecurity Director, Johnson & Johnson Consumer Health

The sixth and final panel discussed supply chain cybersecurity considerations in the CSF.

The panel members and participants in Slack discussed the importance of organizations having a robust cybersecurity supply chain risk management approach, including how CSF 2.0 could build on the coverage of cybersecurity supply chain risk management already included in CSF 1.1. They addressed the many challenges associated with cybersecurity supply chain risk management, including the ability to oversee cybersecurity of suppliers, and emphasized the importance of maintaining flexibility to tailor activities based on risks, sectors, and circumstances. The panel and Slack participants also discussed recently issued resources to help secure software supply chains, such as the NIST Secure Software Development Framework Version 1.1 (NIST SP 800-218) and Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (NIST SP 800-161 Rev. 1). Some panel members also pointed to the importance of global discussions on supply chain management.

NIST's Next Steps

The workshop provided NIST with valuable feedback. This stakeholder input is essential for the open, transparent process to update the Framework. Each step of the process toward CSF 2.0 will build on the previous actions and information—and will inform other NIST activities beyond the CSF update. This workshop was informed by RFI comments and reflected the RFI analysis. Next, NIST will release and seek public feedback on CSF 2.0 concept papers that will be based on several of the themes identified in the RFI comments. For each theme, the concept papers will explain what NIST has heard from stakeholders, including in the RFI comments and the workshop, and offer potential ways to address those issues in a future draft of CSF 2.0.

For more information on the update to the Framework, please visit the NIST CSF 2.0 website. Some ways to engage in the update process include:

- **Visit our website.** Visit the CSF website for updates, upcoming events, resources, and other opportunities to weigh in.
- **Join us at an upcoming workshop.** This was our first workshop in the CSF 2.0 update process. NIST intends to hold additional events to identify specific updates to the CSF. They will be announced on the CSF events page.
- **Submit comments on the CSF.** NIST intends to post at least one draft of the Framework for public comment. Please submit input on what we get right, and most importantly, what we can improve in the draft.

- **Submit a Success Story or resources**. NIST welcomes submissions for CSF Success Stories, Resources, and Perspectives pages. NIST also encourages sharing example CSF profiles focusing on sectors, technologies, or individual organizations.
- **Contribute to the National Online Informative Reference Program (OLIR).** NIST welcomes contributions to OLIR to facilitate informative references (or mapping) between the NIST CSF and other guidance and resources.
- **Follow and engage in our international efforts.** The CSF has been translated and adapted throughout the world, and international stakeholder participation will be critical to the update process. Check out the various international adaptations and translations of the CSF and other NIST cybersecurity and privacy resources, as well as updates on our international engagement and how to get involved at the International Cybersecurity and Privacy site.
- **Meet us at a cybersecurity conference**. NIST staff participate in conferences around the world to increase awareness of the CSF and the update process, as well as learn how organizations are using it. See where we will be participating on the CSF events page.
- **Participate in a NIST forum or community of interest**. NIST will be leveraging several existing forums on the CSF update. Forums can be found on our cybersecurity and privacy stakeholder engagement page.
- **Email Updates.** To receive updates on the CSF, sign up for email alerts via the Email Subscription page.
- **Contact us.** NIST always welcomes questions and suggestions at cyberframework@nist.gov.