ISPAB
NIST Updates to the Cybersecurity Framework

Cherilyn Pascoe | Senior Tech Policy Advisor & Lead, NIST CSF Program
Adam Sedgewick | Senior IT Policy Advisor
July 13, 2022
Journey to Cybersecurity Framework 2.0

• NIST has begun the process of updating the Cybersecurity Framework.

• The update will address the evolving cybersecurity risk and standards landscape and make it easier for organizations to address risks.

• NIST is actively relying on and seeking diverse stakeholder feedback in the update process.

• Ways to engage: https://www.nist.gov/cyberframework
Cybersecurity Framework History

• February 2013 | Executive Order 13636: Improving Critical Infrastructure Cybersecurity

• February 2014 | CSF 1.0

• December 2014 | Cybersecurity Enhancement Act of 2014 (P.L. 113-274)

• May 2017 | Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (CSF required for federal agencies)

• April 2018 | CSF 1.1

• April 2022 | NIST RFI on CSF Update Closed

• Future | CSF 2.0
In February, NIST launched a RFI to solicit input on its cybersecurity resources, including relationship of the CSF with other resources.

- **Cybersecurity Framework**
  - Use of and potential updates to the NIST Cybersecurity Framework (CSF).

- **Cybersecurity Resources**
  - Feedback on NIST cybersecurity resources, including relationship of the CSF with other NIST and other resources.

- **Supply Chain Cybersecurity**
  - The National Initiative for Improving Cybersecurity in Supply Chains.

All comments publicly available: https://www.nist.gov/cyberframework
RFI Analysis

• Received more than 130 RFI responses.
• In June, NIST reviewed the comments and published RFI Summary Analysis.
• Comments fall across 7 themes.
Theme 1: Focus on maintaining and building on the key attributes of the CSF with the update.

- Subthemes: 1.1 The CSF is widely used and effective in helping organizations understand and manage cybersecurity risks.
- 1.2 The flexible and voluntary nature of the CSF has been beneficial for implementation by organizations of varying sizes and capabilities.
- 1.3 Ensure the CSF is simple and easy to use.
- 1.4 Keep the CSF effective in enhancing communication with non-IT and security stakeholders, including the C-suite.
- 1.5 Maintain backwards compatibility.
Theme 2: Align the CSF with existing efforts by NIST and others.

- Subthemes: 2.1 Align the CSF with recent NIST efforts reflected in a variety of resources.
- 2.2 Make it easier to understand how the CSF can be used with other cybersecurity guidance; provide more mappings with the NIST National Online Informative References Program (OLIR) and Informative References.
- 2.3 Address the important role of governance in cybersecurity risk management, although there are several different approaches for doing so.
- 2.4 Improve alignment between the CSF and NIST privacy resources.
- 2.5 Engage with other federal agencies to ensure effective use of the CSF for policy, legal, and regulatory purposes.
- 2.6 Increase international collaboration and engagement, including alignment with the ISO 27000 series.
Theme 3: Offer more guidance for implementing the CSF.

- Subthemes: 3.1 Offer more guidance on CSF implementation.
- 3.2 Provide specific guidance on developing CSF profiles.
Theme 4: Ensure the CSF remains technology neutral but allows it to be readily applied to different technology issues – including new advances and practices.

- Subthemes: 4.1 Ensure the CSF remains technology neutral while providing guidance on how it is used to address cybersecurity risks in IT, OT, and IoT.
- 4.2 Consider the importance of software security, either as part of the CSF or in conjunction with the CSF.
- 4.3 Ensure the CSF remains technology neutral yet can be applied to specific and emerging topics; such as cloud, hybrid work, and zero trust.
Theme 5: Emphasize the importance of measurement, metrics, and evaluation in using the CSF.

- Subthemes: 5.1 Consider and highlight how the CSF is used as an assessment tool, including when to consider additional guidance on assessment (for self, suppliers, products, and services).
- 5.2 Provide a means to measure CSF implementation.
- 5.3 Expand on (or, in contrast, remove) Tiers and include (or do not include) guidance on maturity models.
Theme 6: Consider cybersecurity risks in supply chain in the CSF.

- Subthemes: 6.1 Address supply chain risks, either in the CSF or separately.
• Theme 7: Use the National Initiative for Improving Cybersecurity in Supply Chain (NIICS) to align practices and provide effective practices, guidance, and tools to bolster cybersecurity supply chain risk management.

  • Subthemes: 7.1 Align cybersecurity supply chain risk management practices, including federal activities and resources.
  • 7.2 Offer more guidance on component inventories; such as software bill of materials and hardware bill of materials.
  • 7.3 Engage on open-source software security issues.
  • 7.4 Offer more guidance on supplier relationship management and contracts.
  • 7.5 There are opportunities for NIICS to research, analyze, and develop tools and techniques for better managing cybersecurity risks in supply chains.
CSF Update Next Steps

- NIST will rely on significant stakeholder feedback to inform the update.
  - Discussion will focus around the RFI themes
  - Direct engagement with stakeholders
  - Public workshops – in-person and virtual
  - Comment on CSF 2.0 draft
  - Continuing to seek and develop CSF resources, success stories, mappings to other frameworks and standards
Update on NIST CSF Resources

Recently published:

• Ransomware: Ransomware Risk Management: A Cybersecurity Framework Profile (NISTIR 8374)
• March White House Fact Sheet: Cybersecurity Framework Profile: White House Fact Sheet (by Seamless Transition)

In draft:

• PNT: Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (NISTIR 8323 Rev. 1) (Draft) – comments open now
• Satellite Ground: Applying the Cybersecurity Framework to Assure Satellite Command and Control (NISTIR 8401) (draft)
• Hybrid Satellite Networks: Cybersecurity Profile for the Hybrid Satellite Networks (HSN) Cybersecurity (draft outline) – comments open now
• LNG (with DOE): Cybersecurity Framework Profile for Liquefied Natural Gas (draft)
• Elections: Cybersecurity Framework Election Infrastructure Profile (NISTIR 8310) (draft)
Update on CSF International

- Translated into Japanese, Spanish, Portuguese, Arabic, Bulgarian, Polish, Indonesian, French, Ukrainian.
- Adapted into national cybersecurity policies, strategies, and requirements.
- Use cases identified in all regions.