March 15, 2023

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899-2000
Email: cyberframework@nist.gov

Re: Comments on the NIST CSF 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

Fortinet, Inc. (Fortinet) [1] respectfully submits these comments in response to the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework (CSF or Framework) 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework (hereinafter "CSF 2.0 Concept Paper") released January 19, 2023.[2] Fortinet welcomes NIST's efforts to seek feedback on the NIST CSF 2.0 Concept Paper to inform further development of CSF 2.0 and offers the following comments with respect to NIST's potential significant changes and associated questions.

Background

Founded in 2000, Fortinet is a US-based developer of novel and next generation security and networking solutions and architectures. Holding more than 1,250 patents, Fortinet is the most innovative provider of cybersecurity and is focused on protecting the breadth of the digital attack surface from edge to core to cloud. Fortinet leverages analytic expertise, artificial intelligence, and machine learning systems to analyze security events to protect against ransomware, malware, and other threats. Fortinet secures over half a million enterprises, service providers, and government organizations around the world.

1.1 Change the CSF's title and text to reflect its intended use by all organizations

Fortinet applauds the change of name from "Framework for Improving Critical Infrastructure Cybersecurity" to "Cybersecurity Framework" to more accurately reflect

[1] Fortinet, Inc. (NASDAQ: FTNT) is a US-based developer of custom cybersecurity solutions that assists governments, service providers, and hundreds of thousands of businesses around the world to secure their networks and drive digital innovation. For more information, see www.fortinet.com.

[2] NIST CSF 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework, January 19, 2023, https://www.nist.gov/system/files/documents/2023/01/19/CSF_2.0_Concept_Paper_01-18-23.pdf.

common usage. However, in our experience many organizations, especially small and midsize businesses lacking cybersecurity expertise, do not recognize at the outset that the CSF serves as a framework for risk management. In some cases, this leads organizations to believe, for example, that the Framework is focused on threats to cybersecurity and that the "identity" function refers to threat activity and not to identification and prioritization of enterprise assets for protection. To more accurately capture the scope and purpose of the CSF, we would suggest that a title such as "Cybersecurity Risk Management Framework" could be used to better signal the document's purpose to industry, even if it does not reflect common usage.

1.2 Scope the CSF to ensure it benefits organizations regardless of sector, type, or size

Fortinet applauds the explicit recognition that consumers and users of the CSF include higher education institutions and state/local government. Local government in particular is chronically short of cybersecurity talent, especially in areas such as procurement and contract/project management. We would recommend that the linkage of resources in CSF 2.0 include links to exemplar contract language for functions or activities identified in the Framework. A considerable body of relevant contract language is produced by the Federal Government (the Cybersecurity and Infrastructure Security Agency, General Services Administration, Office of Management and Budget guidance, etc.) and could be housed either within the U.S. Government or by a third party (a Federally Funded Research and Development Center, non-profit organization, university, etc.) for access by the public.

1.3 Increase international collaboration and engagement

While the CSF has evolved in scope and intended audience from version 1.0 to 1.1 and prospectively to 2.0, the reality is that as a publicly available document that presents a coherent, comprehensive, and technology-neutral approach to cybersecurity, it has always had a significant international user population. Recognizing this in CSF 2.0 and allowing for relevant regional variation in implementation reference links would help to make it actionable for a broader array of users, as for example, when differing regimes on data sovereignty might apply to an organization. Allowing for such variation should not automatically make NIST responsible for curating and maintaining their accuracy and relevance; although as an

organization with strong international ties NIST would certainly be a valuable conduit for such information.

2.6 Remain technology- and vendor-neutral, but reflect changes in cybersecurity practices

Fortinet believes that the focus of the CSF since its inception on technology and vendor-neutral outcomes is a large part of what has made the Framework successful, but we agree that it should be updated to reflect and leverage broad changes in cybersecurity such as the growing maturity and adoption of Zero Trust Architectures and operating principles. Similarly, the growing focus on Supply Chain Risk Management (SCRM) should be reflected in a manner that articulates its importance and contains references to key U.S. Government, private sector, and international standards and programs. In addition, individual organizations and consortia of organizations are increasingly focusing on security orchestration and response and on coordinated incident handling. The growing importance and resources available in these areas should likewise be reflected in CSF 2.0.

3.1 Add implementation examples for CSF Subcategories

Fortinet applauds the inclusion of notional implementation examples to help readers understand how to achieve the outcomes described in the CSF. Our experience with both CSF 1.0 and 1.1 was that users with limited experience in cybersecurity often found them readable but abstract and not readily actionable. Providing a small number of exemplar use cases, written to cover a wide variety of approaches and solutions, would help readers orient their thinking. We believe that these exemplars should be included in the CSF 2.0 Core document since this would help to maximize its utility as a free-standing document. When appropriate, such notional exemplars could point to CSF case studies, use cases, success stories, and example profiles.

3.2 Develop a CSF Profile template

Fortinet agrees that developing CSF profiles for specific sectors and types of users can help organizations get started with or improve their use of the CSF, and Fortinet looks forward to working with NIST to help build out this type of content.

4.1 Add a new Govern Function

Fortinet applauds the addition of "Govern" as a Functional level element. Without oversight and steerage, cybersecurity and security risk management policies are often ad hoc and reactive. Given the rise of the role of a Chief Data Officer (CDO) within many organizations and the proposed linkage of security to privacy (see Section 2.3 on Cybersecurity and Privacy reference tool), we believe that this function should include a discussion of data governance roles and responsibilities.

5.1 Expand coverage of supply chain

As noted previously in comment 2.6, Fortinet believes that SCRM is critically important to cybersecurity and should be reflected in terms that capture the breadth of challenges (*e.g.*, hardware, software, producers, users, etc.) but present them in actionable terms. Too many efforts to address SCRM have presented it as an intractable and unmanageable problem or end in "paralysis by analysis."

We applaud the linkage to actions being undertaken to implement Executive Order 14028 such as the Software Bill of Materials efforts and agree that elements of SCRM should be reflected in multiple functions and categories of CSF 2.0.

6.0 CSF 2.0 will advance understanding of cybersecurity measurement and assessment

Cyber measurement and assessment is often undertaken to answer one of three types of questions:

- How secure is my organization? (*i.e.*, establish a baseline of performance)
- How can I prove it? (*i.e.*, demonstrate compliance or performance certification)
- How can my organization improve its security? (*i.e.*, gap analysis and change management)

These three types of measures are different, and in practice, measuring compliance often consumes most of the relevant measurement resources for an organization. To offer guidance on this issue, CSF 2.0 should reference the numerous and varied approaches to baselining performance. In addition, we encourage NIST to focus on the third question—helping organizations focus on security improvement—since this is arguably the ultimate goal of the CSF. Fortinet believes there are existing approaches and tools that can facilitate gap analysis and help organizations measure aspects of their security under varying operating

conditions, and we would be willing to contribute to the creation of CSF resources such as use cases or example profiles for actionable performance measurement.

Conclusion

NIST's CSF 2.0 Concept Paper serves as a valuable opportunity for organizations to offer feedback and recommendations on CSF changes. Fortinet supports NIST's efforts to make substantial changes with CSF 2.0, ensuring it reflects the evolving cybersecurity landscape. We stand ready to work with NIST and other stakeholders to further assist in updating CSF 2.0. We also appreciate the opportunity to provide our input and your attention to these comments.

Respectfully submitted,

James Richberg, Public Sector CISO
Fortinet, Inc.