wiley

ALERT

Cybersecurity Framework: Updates Coming as Expectations Rise

May 19, 2017

The National Institute of Standards and Technology (NIST) held a public workshop on Tuesday and Wednesday in Gaithersburg, Maryland to discuss proposed updates to its highly-lauded *Cybersecurity Framework for Critical Infrastructure* (CSF), which was released in 2014. CSF Draft Version 1.1 was released on January 10, 2017, and NIST has taken public comment. A summary by NIST of the comments received is available here. Major issues emerging for NIST and industry to tackle include whether and how to measure cyber success, whether to include "bug bounty" or coordinated vulnerability disclosures, how to address the Internet of Things (IoT), and how to harmonize the CSF with the recent presidential Executive Order on Cybersecurity, which mandates federal agency use of the CSF.

A panel of private sector participants discussed their use of the CSF as a tool to discuss cybersecurity throughout their organizations and with their partners. It was seen as a positive contribution to the private sector broadly, which is increasingly using the CSF to shape internal risk management and evaluations. International commenters described non-U.S. governments' reactions to and reference to the CSF. They urged the United States to continue and increase its advocacy on the global stage to promote harmonization when it comes to cybersecurity best practices and expectations.

Below is a high-level read-out on some of the key issues that NIST is working through for Version 1.1:

- **Metrics:** The workshop revealed nearly global consensus that the topic of metrics is critically important. However, workshop participants voiced concern about NIST's treatment of the topic in Version 1.1. Generally, participants urged NIST to simplify

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

Telecom, Media & Technology

the metrics section and to reevaluate the level of detail that NIST provides regarding metrics. Workshop participants agreed that more work needs to be done with research around metrics, and that the final product needs to maintain flexibility.

- **Coordinated Vulnerability Disclosures:** Workshop participants affirmed that this is a mature topic that is ready for inclusion in the CSF. Participants also suggested additional research into the intersection between coordinated vulnerability disclosures and the CSF.
- **Law and Policy:** Participants noted that the CSF is widely used and may become a standard of care. They also expressed concern about the potential for regulation or misuse, which might be in tension with federal policy and law on cybersecurity. They highlighted that the voluntary nature of the CSF is what makes it successful, and suggested further engagement with regulators—at both the federal and the state level—to ensure that they understand the CSF's voluntary nature.
- **Supply Chain:** Participants agreed that clarifying language is needed at the beginning of the supply chain risk management (SCRM) section to further explain context and complexity. Although NIST was receptive to written comments urging it to not make SCRM its own category and to instead incorporate SCRM into the existing categories; it ultimately came to the conclusion at the workshop that such integration would be more appropriate for Version 2.0. For the current Version 1.1, NIST plans to keep SCRM as its own category.
- **Authentication:** Generally, workshop participants affirmed that the new authentication language proposed in Version 1.1 is appropriate and strengthens the overall category. Based on consensus from participants, NIST plans to add an authentication subcategory. With this subcategory, NIST hopes to provide examples of authentication tools, but not drive organizations to certain solutions that may not make sense for their particular needs or risk profiles. To do this, NIST proposed identifying several authentication tools as options.
- **Threat Intelligence**: Participants suggested modifying the Core Framework language to specifically call out threat intelligence.

Additionally, workshop panelists and attendees considered the application of the CSF to certain areas, including the Communications Sector and IoT.

- **Communication Sector:** The Communications Sector panel and discussion group highlighted the CSRIC mapping efforts, and focused mainly on metrics. The overall recommendation coming out of this discussion was that the metrics section in Version 1.1 should be streamlined at a higher level, and that additional work needs to be done looking at metrics that focus on organizations' internal risk management processes. The panel also warned that complex metrics may drive away potential users of the CSF. They highlighted that any metrics need to be understandable to the audience. Finally, the panel warned against tying metrics to CSF subcategories.
- **IoT:** This discussion highlighted the vast IoT ecosystem, which is made up of many actors (e.g., device manufacturers, network providers, enterprise, consumers, etc.) across all sectors. With this context, discussion revolved around the intersection of the CSF with IoT. While there was general consensus that the CSF as a tool is applicable to IoT, there was much discussion about how best to use that tool.

> Suggestions included sector profiles, threat profiles, use cases, and including IoT into the CSF itself, among others. There was a suggestion that NIST might be able to add value to the IoT cyber effort at the consumer level, as there is little guidance/few standards regarding in-home and consumer IoT devices, as compared to enterprise IoT devices.

Going into the workshop, NIST had predicted that it would have the final version of 1.1 complete by the Fall of this year. Following the workshop, NIST introduced the idea that it may publish another draft before moving to a final version. We can expect a decision to be made public in June or July, along with a summary of the workshop.

***

Wiley Rein has been actively engaged with NIST on cybersecurity for years, including its previous implementation of President Obama's Executive Orders on cybersecurity. We have advised numerous companies on how evolving expectations about cyber will impact them, from regulatory obligations to consumer communications, and government contract provisions.

We are happy to answer questions you may have.