wiley

NEWSLETTER

NIST Moves to Update its Cybersecurity Framework, Seeks Public Comment

March 2022

Privacy In Focus®

The National Institute of Standards and Technology (NIST) has kicked off the process for revamping its flagship cybersecurity guidance document – the Framework for Improving Critical Infrastructure Cybersecurity (CSF), which is now several years old. Specifically, on February 22, 2022, NIST published a Request for Information (RFI) related to evaluating and improving the CSF. NIST intends to make the CSF a more valuable tool in the quickly evolving threat landscape. The RFI also seeks input from the public to inform the direction of its newly launched National Initiative for Improving Cybersecurity in Supply Chains (NIICS), including how it might be aligned and integrated with the CSF. Comments on the RFI are due by April 25.

NIST's fresh look at the CSF is one of several efforts underway across the federal government to address cybersecurity. And as more regulatory approaches to cybersecurity are emerging, and as NIST delves into privacy risk management, NIST's consensus-based and voluntary approach to cybersecurity is more important than ever for companies to pay attention to. Below, we provide details on the CSF, as well as NIST's current effort to refresh it and expand its supply chain cybersecurity efforts. Wiley's Privacy, Cyber & Data Governance Team has helped entities of all sizes and sectors proactively address their cybersecurity risks and advocate before government agencies, including NIST, on cybersecurity policy and guidance. For more information on NIST's new RFI, please reach out to any of the authors of this article.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Privacy, Cyber & Data Governance

NIST's Cybersecurity Framework

The CSF, which is voluntary for the private sector, provides guidance and a framework for organizations of all types and sizes to assess and manage cybersecurity risks. It consists of standards, methodologies, procedures, and processes that help users align policy, business, and technological approaches to reduce cybersecurity risks for critical infrastructure, as well as other organizations across both the government and private sector.

NIST first released CSF V1.0 in 2014 in response to Executive Order 13636, which directed NIST to collaborate with stakeholders to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure. NIST later updated the CSF in 2018 with CSF V1.1, to provide a more comprehensive approach to identity management and supply chain cybersecurity. Throughout NIST's development of the CSF, it has actively sought feedback from the public and engaged with stakeholders. These efforts include public workshops, requests for information, and requests for comment on draft versions of the CSF. NIST's work on the CSF has been lauded as an example of the ideals of public-private collaboration.

The CSF has become a model for other work, including NIST's effort on supply chain and privacy, as well as work by other agencies on cyber performance goals for critical infrastructure. Third-party standards have built on it, and other countries have incorporated its structure into their own critical infrastructure regimes.

The National Initiative for Improving Cybersecurity in Supply Chains

The NIICS was recently launched by NIST and will serve as a public-private partnership that will seek to address cybersecurity risks in supply chains by focusing on identifying tools and guidance for technology developers and providers. NIST believes that the NIICS will also help address a need for organizations acquiring technology products and services to utilize practical, performance-oriented guidance to address broader cybersecurity risks to the security and resilience of all supply chains. NIST may issue a future RFI to further guide this partnership.

Request for Information

In the RFI, NIST writes that the cybersecurity landscape has changed significantly since CSF V1.1 was released nearly four years ago, particularly with respect to threats, capabilities, technologies, education and workforce, and the availability of resources to help organizations to better manage cybersecurity risk. Additionally, there now exists an increased awareness of cybersecurity risks in supply chains, according to NIST. We at Wiley have seen this evolution over more than 10 years, helping clients invest and mature their risk management approaches, iterate response plans, and reevaluate governance. Many clients rely on the CSF, alongside other standards – both from NIST and from industry and third-party groups.

Recognizing that approaches have matured, but also that there are still gaps to be addressed, the RFI seeks information to help the identification and prioritization of cross-sector supply chain-related cybersecurity needs. NIST also seeks to gain a better understanding of the degree to which other NIST resources are used in conjunction with the CSF.

The RFI includes a non-exhaustive list of 14 questions, as outlined below.

Questions 1-6 – Use of the CSF: The first six questions seek feedback about the utility of the CSF, including the benefits and challenges of implementing the CSF and whether its structure or features should be modified.

Questions 7-10 – Relationship of the CSF to Other Risk Management Resources: Questions 7-10 focus on how the CSF fits into the broader cybersecurity risk management ecosystem, including ways to integrate the CSF with other NIST and non-NIST cybersecurity resources and steps that could increase international use of the CSF.

Question 11 – NIICS: Question 11 focuses on the NIICS and seeks information on current cybersecurity supply chain risk management (C-SCRM) challenges and how the NIICS can be leveraged to increase trust and assurance in technology products, devices, and services.

Questions 12-13 – C-SCRM Resources: Questions 12 and 13 seek input on resources that are necessary for managing supply chain cybersecurity risks – including how they apply to information and communications technology, operational technology, the Internet of Things (IoT), and industrial IoT – and whether there are any gaps in these existing resources that NIST could address.

Question 14 – Integration of CSF and C-SCRM Guidance: The final question focuses on whether and how C-SCRM considerations could be integrated into the updated CSF or whether a new, separate framework focused on C-SCRM would provide more value.

February Workshop on the CSF and the RFI

On February 24, 2022, the National Cybersecurity Center of Excellence at NIST held a fireside chat titled *A Look at the Cybersecurity Framework: Where We've Been, Where We Are, and Where We're Going*. The event featured two NIST representatives for a facilitated Q&A on the past, current, and future state of the CSF. The event began with an overview of the evolution of the CSF and how the CSF has been applied to improve cybersecurity both domestically and internationally. The Q&A then shifted to the RFI. Among other things, the NIST representatives discussed NIST's plans to hold workshops on the CSF following the close of the public comment period and indicated that it may provide an updated timeline on the release of the updated CSF at that time.

What Should the Private Sector Do?

Now is the time to tell NIST about organizations' use of the CSF alongside other standards and approaches. NIST welcomes input on the diversity of approaches, costs and benefits, and challenges and opportunities. As federal cyber policy hits a major fork in the road in choosing regulation or partnership, NIST can play an important role to inform policymakers and maintain the best aspects of public-private collaboration on cyber challenges facing the economy.

We urge private companies to:

- Review their current use of the CSF and other NIST publications.
- Identify what NIST can do to clarify and better support diverse private organizations in their cyber risk management.
- Consider participating in the NIST proceeding to ensure broad and diverse feedback can inform this next iteration of this important document.

Comments on this RFI are due April 25, 2022. There will be future opportunities to comment, but we have found that early input to NIST can be particularly helpful as the agency shapes drafts and its work.