wiley

NEWSLETTER

Industry Highlights NIST Cybersecurity Framework's Value as NIST Weighs a Potential Update

May 2022

Privacy In Focus®

Public comments in an ongoing cybersecurity proceeding at the National Institute of Standards and Technology (NIST) highlight the utility of a foundational cybersecurity document while also providing suggestions for its improvement. NIST has begun to evaluate the 130 comments it received in response to its Request for Information (RFI) related to evaluating and improving its flagship cybersecurity guidance document, the Framework for Improving Critical Infrastructure Cybersecurity (CSF). NIST is seeking to determine whether and how to update the CSF, which is used widely across the globe by organizations of all sizes. The RFI also sought comment on NIST's National Initiative for Improving Cybersecurity in Supply Chains (NIICS) – a new public-private partnership that will seek to address cybersecurity supply chain risk management (C-SCRM) issues – as well NIST's other C-SCRM efforts.

Commenters and Consensus

The record reflects a diverse group of participants, including trade associations, industry coalitions, individual companies, standards organizations, and security vendors. Several federal agencies also submitted comments, including the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Aviation Administration (FAA), and the U.S. Department of Energy.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Practice Areas

Cyber and Privacy Investigations, Incidents & Enforcement

Cybersecurity

Privacy, Cyber & Data Governance

The record reflects a general consensus that the CSF is relied upon heavily and that significant changes would be disruptive to its usability and longevity. Many organizations discussed the CSF's utility as a flexible, voluntary, and risk-based document that can be applied in a variety of different use cases. Indeed, it is critical that companies pay attention to the CSF's consensus-based and voluntary approach to cybersecurity as the federal government pursues new regulatory approaches to addressing cybersecurity risks.

Suggested Changes

Beyond the general agreement on the CSF's utility, the record reflects a wide range of suggestions, both for improving the CSF and for guiding the NIICS. Several commenters sought targeted changes to the CSF. For example, several communications and technology trade associations recommended that NIST update the Informative References that it provides on its Informative Reference Catalog and map the CSF to additional frameworks, regulations, and standards. With respect to the NIICS, many commenters recommended that NIST coordinate and harmonize its C-SCRM efforts with other ongoing federal C-SCRM initiatives.

Certain commenters sought more extensive changes to the CSF. For example, a few commenters sought significant changes to the C-SCRM portion of the CSF, including changes to the CSF's Categories and Subcategories. However, many of the commenters who addressed C-SCRM discouraged NIST from building a new C-SCRM framework separate from the CSF. Several individual companies and security vendors suggested incorporating more metrics into the CSF, while others recommended adding more privacy and data protection elements to the CSF.

NIST plans to hold additional workshops to gain further perspectives on potential changes to the CSF. It is likely that NIST will also release public drafts of the updated CSF, which would provide additional opportunities for the public to provide feedback. Wiley's Cyber and Privacy Investigations, Incidents & Enforcement team has helped entities of all sizes and sectors proactively address their cybersecurity risks, including through advocacy at NIST. If you would like more information on this proceeding, please reach out to any of the authors of this article.