NIST is Seeking Public Advice to Help Cybersecurity for the Supply Chain

Article By

Peter Vogel

Foley & Lardner LLP

Related Practices & Jurisdictions

- Communications, Media & Internet
- Administrative & Regulatory
- Utilities & Transport
- All Federal

Friday, March 25, 2022

NIST issued a Request for Information (RFI) “seeking information to assist in evaluating and improving its cybersecurity resources, including the “Framework for Improving Critical Infrastructure Cybersecurity” (the “NIST Cybersecurity Framework,” “CSF” or “Framework”) and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. NIST is considering updating the NIST Cybersecurity Framework to account for the changing landscape of cybersecurity risks, technologies, and resources.” The February 22, 2022 RFI is entitled “Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management” which includes these important points:

NIST recently announced it would launch the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains.
This wide-ranging public-private partnership will focus on identifying tools and guidance for technology developers and providers, as well as performance-oriented guidance for those acquiring such technology.

To inform the direction of the NIICS, including how it might be aligned and integrated with the Cybersecurity Framework, NIST is requesting information that will support the identification and prioritization of supply chain-related cybersecurity needs across sectors.

Responses to this RFI will inform a possible revision of the Cybersecurity Framework as well as the NIICS initiative.

Please submit your comments to NIST by April 25, 2022.

© 2022 Foley & Lardner LLP

Source URL: https://www.natlawreview.com/article/nist-seeking-public-advice-to-help-cybersecurity-supply-chain