From: Jennifer Kurtz
Sent: Monday, April 25, 2022
To: CSF-SCRM-RFI
Cc: Paulsen, Celia (Fed)
Subject: RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.

Dear NIST Team,

Thank you for inviting public comment on “RFI: Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.” I reference the CSF in my conversations and briefings to clients, both those within the DoD/aerospace supply chain and those outside that and other more highly regulated manufacturing industry sectors. It's simple to grasp and yet subtle to achieve. Here are my comments:

- For manufacturers, I believe it would be helpful to have cybersecurity principles and controls expanded or explained using quality management or OSHA terminology. This would help demystify cybersecurity guidance and lower the barrier to understanding and acceptance. It would also encourage service providers to think like manufacturers rather than like advocates for a specific technical solution.
- Incorporate the look and feel of NIST HB 162 in a companion piece. The ideas and comments published emphasize the need for connecting the dots between control statement and real-world implementation. More manufacturing and other implementation scenarios would be helpful.
- Include in the guidance references to reading legal documents pertaining to third-party service providers, cyber insurance riders, and the like. When I ask cyber or business leads about the contract terms the response is often "I'll have to look."
- I still would love to see states include cybersecurity information and the requirement for both a system security plan and incident response plan as part of the business registration process. It would not be complicated to include templates for policy documents and plans on the state web portal.
- Expand the discussion of an IT asset register to include a data repository analysis that looks at all the business information system resources and identifies the level of interest, as it were, in terms of data criticality (to the business' survival), data sensitivity (this would include notes about PHI. PII, ITAR, CUI, etc. and whether it is rated as high/medium/low for a given characteristic), and data recoverability. (*Reference:* NIST SP 800-61r2)
- The specific and well-developed comments from Gideon Rasmussen are superb.

Thank you and good luck on this important work,

Jennifer

Jennifer Kurtz, MBA, PMP
Cyber Program Director
Author, *Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking*
US DEPARTMENT OF COMMERCE:
NIST MANUFACTURING EXTENSION PARTNER