Federal Cybersecurity and Privacy Professionals Forum Meeting
National Institute of Standards and Technology
March 24, 2022

NIST Cybersecurity RFI Feedback Session for Forum Members

March 24, 2022, 1:00 PM ET – 2:30 PM ET

1:00 PM – Welcome and Announcements – Victoria Pillitteri (Forum Co-Chair, NIST) and Kaitlin Boeckl (Forum Co-Chair, NIST)

Presentation from NIST on Cybersecurity RFI – Kevin Stine (Chief Cybersecurity Advisor, NIST)

Open Discussion with Forum Participants on Cybersecurity RFI – All forum participants, moderated by Kevin Stine (Chief Cybersecurity Advisor, NIST), Cherilyn Pascoe (Senior Technology Policy Advisor), Jon Boyens (Deputy Chief, Computer Security Division), Adam Sedgewick (Senior Technology Policy Advisor), Amy Mahn (International Policy Specialist, Applied Cybersecurity Division), Angela Smith (Computer Security Division)

NIST would like to hear from the Forum participants on the improvements to its resources as called for by the Cybersecurity RFI. NIST will facilitate a discussion with Q/A and feedback from Forum participants. *Please use the "raise hand" function in WebEx to be called on to provide input.

1. **Feedback on updates to the NIST Cybersecurity Framework**
   a. How are Forum participants using the Cybersecurity Framework?
   b. Has the CSF improved communication within your organization?
   c. What challenges have prevented organizations from using the CSF more effectively?
   d. Any other suggestions on areas of improvement to the CSF?

2. **Feedback on harmonization of NIST cybersecurity resources and the CSF**
   a. NIST also wants to explore better ways to align the CSF with other NIST guidance, such as the Privacy Framework, Secure Software Development Framework, Risk Management Framework, NICE Workforce Framework, and its series on IoT cybersecurity. How are Forum participants using these NIST cybersecurity resources separately as well as combined with the CSF?
   b. Are there non-NIST cybersecurity resources/frameworks/guidance that Forum participants are using that you find useful?
   c. Any suggestions for improvements to reduce conflicts?

3. **Feedback on NIST's efforts on supply chain cybersecurity, including the National Initiative for Improving Cybersecurity in Supply Chains (NIICS)**
   a. What are the gaps in existing cybersecurity supply chain risk management guidance and resources, including how they apply to open source software, operational technology, IoT, and industrial IoT?
   b. How can NIST build on its current work on supply chain security, including software security work stemming from Executive Order 14028, Improving the Nation's Cybersecurity, to increase trust and assurance in technology products and services?

Closing Remarks – NIST

2:30 PM – Meeting Adjourned