Life Is On | Schneider Electric

Dr. Laurie Locascio<br>
Under Secretary of Commerce for Standards and Technology and Director<br>
National Institute of Standards and Technology<br>
100 Bureau Drive<br>
Gaithersburg, MD 20899

April 25, 2022

**RE: Request for Information on Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management**

Dear Dr. Locascio:

Schneider Electric strongly supports the National Institute of Standards and Technology (NIST) update of its resources on cybersecurity. As a critical manufacturer with operations in over 100 countries, we actively leverage both the NIST Cybersecurity Framework and NIST's supply chain security resources to ensure the cybersecurity of our assets, solutions, and customers.

At Schneider Electric, we drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

Our integrated solutions enable homes, commercial buildings, data centers, and critical infrastructure to operate more efficiently and securely. Our products and systems are used in over one million buildings worldwide, including 40,000 water & wastewater treatment installations, 40% of the world's hospitals, 10 of the world's top electric utilities, and 10 of the world's largest airports. The cybersecurity of these products and systems is therefore of vital importance to us and our customers. As such, Schneider Electric is an active participant in the cybersecurity community in the U.S. and abroad. Below are selected examples of our engagement:

- World Economic Forum Centre for Cybersecurity Partner
- Paris Call for Trust and Security in Cyberspace Supporter
- Cyber Tech Accord Signatory
- Cybersecurity Coalition Member
- ISA Global Cybersecurity Alliance Founding Member
- Electricity Information Sharing and Analysis Participating Vendor
- Department of Energy CyTRICS program – first participating manufacturer to test products used in the U.S. grid.
- CISA Industrial Control Systems Joint Working Group (ICSJWG) – we hold multiple leadership positions in relevant working groups.
- Participate in numerous standards development organizations from the International Electrotechnical Commission (IEC) to the International Organization for Standardization (ISO) to craft relevant cybersecurity standards for our products and solutions.

- Schneider Electric, together with the ISA GCA, is working hand in hand with CISA and companies globally to utilize the proven FEMA Incident Command System for use in coordinating cyber incident responses. This effort is called the Incident Command System for Industrial Control Systems (ICS4ICS). This innovative framework helps cyber responders globally to identify, respond, and recovery from cyber incidents using the same framework emergency responders in all other sectors use every day.

Our responses to the RFI questions are listed below:

- At Schneider Electric, we are active consumers of the NIST Cybersecurity Framework (the Framework) and support its continued use and adoption throughout the digital ecosystem.
- In particular, we find the Framework's Core functions of "Identify", "Protect", "Detect", "Respond", and "Recover" very helpful in driving the right conversations around cybersecurity with a broad audience of stakeholders, and we support the continued use of these functions in future versions of the Framework.
- The Framework's international credibility and adoption could be improved if the Framework were to become an international standard. We believe that such an action would not only drive broader global adoption, but could help improve the harmonization of corresponding regulatory requirements from governments throughout the world.
- When the Framework was originally conceived in 2014 and then updated in 2018, much of the cybersecurity community was focused on securing information technology (IT) systems and assets. However, our world has changed a great deal since 2018 and we are seeing a rapid increase in attacks on operational technology (OT), which is used to control physical functions within critical environments. Any future updates to the Framework should take OT security challenges into account and provide detailed guidance to practitioners on how to address these challenges. Specifically, we recommend that NIST conduct a workshop with both IT and OT providers to develop more granular guidance in the updated Framework for IT environments, OT environments, and environments where the two technologies converge.
- In addition to updating the Framework, NIST should consider issuing detailed implementation guidance with a focus on the assessor community. In our experience, there is inconsistency in how third parties assess an organization's alignment to the Framework and that inconsistency can be unhelpful in developing shared understanding of a cybersecurity environment and its maturity.
  - For example, some in the assessor community conflate the Framework Tiers with "maturity levels". Conflating these terms causes confusion within assessed organizations and the broader community.
  - Our recommendation is that NIST continue to stress in such guidance that the Framework is not a maturity model.
  - Such guidance would benefit from discrete examples of how the Framework has been implemented and assessed within specific organizations.
  - Such guidance would need to be updated regularly to reflect current technologies and threats, and would need to be consistent with existing international standards and relevant assessment methodologies (e.g., ISA/IEC 62443 suite and ISO 27000 series).
- In our experience, the Framework would benefit from more robust references and guidance on how to identify and protect against supply chain security threats. Many organizations feel more exposed by their supply chain than by their own organization, products, or systems, and this area of risk should be addressed in a fulsome manner within the Framework.

- Related to supply chain risks, the Framework could be updated with guidance on how to address the challenge of securing open source software and components. Such guidance could include a list of testing tools/resources (e.g., code analysis, fuzz testing, and vulnerability testing) to facilitate improved security of open source software and components.
- The Framework should be updated with informative references to key relevant cybersecurity initiatives that have taken place since 2018. For example, it would be helpful for the Framework to provide granular guidance on how organizations should build and leverage software bills of material to address cybersecurity threats, or in how Zero Trust principles interrelate to the Framework.
- As NIST has done with previous versions, we would appreciate the Framework being updated with relevant informative references (e.g., NIST 800-171, ISO 27000 series, and ISA/IEC 62443 suite) as this mapping facilitates implementation and alignment to multiple relevant standards.
- In general, we encourage NIST to align its definitions in the Framework to existing international standards (e.g., ISO 27000 series and ISA/IEC 62443 suite) to reduce confusion within the community.
- In general, we encourage NIST to use flexible language within the Framework so that practitioners can leverage the Framework for products, systems, and/or systems of systems interchangeably. Flexible language allows practitioners to zoom in or out depending on the relevant use case.

Schneider Electric sincerely appreciates the opportunity to comment on the RFI. If you have any questions or need additional information, please contact me at [redacted]

Sincerely,

Patrick M. Ford

Patrick M. Ford
Regional Chief Information Security Officer, Americas Region
Schneider Electric