April 25, 2022

Via: www.regulations.gov

Ms. Katherine MacFarland
National Institute of Standards and Technology
100 Bureau Drive (Stop 2000)
Gaithersburg, MD 20899

Re: ACC Comments- NIST Cybersecurity RFI

Dear Ms. MacFarland:

The American Chemistry Council's (ACC) Chemical Information Technology Center (ChemITC) submits the following comments regarding the chemical sector's experience with the Cybersecurity Framework. ChemITC supports the framework and its continuing flexibility. The framework is complimentary to the voluntary Security Code included into ACC's Responsible Care® Program and other voluntary frameworks that have similar goals. ChemITC has actively promoted the National Institute of Standards and Technology (NIST) cybersecurity framework (the framework) since it was released in 2014. The framework is backed by many industry sectors, and the proposed updates, especially provisions related to the supply chain, generally represent enhancements to the original framework.

Our experience indicates that the framework is extremely useful. ChemITC members are using the framework and urging business partners to do the same to better manage cybersecurity risks to their information networks and systems. We believe any proposed enhancements to the framework are likely to encourage greater implementation across industry sectors and particularly within an industry supply chain. We also believe that major changes to the framework are not needed.

Standards, guidance, and best practices relevant to cybersecurity are typically industry-driven and adopted on a voluntary basis, and they are most effective when developed and recognized globally. Such an approach avoids burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions. The NIST framework continues to provide this kind of helpful global model to adopt.

To augment existing programs within ACC, ChemITC prepared guidance to implement the cyber related activities under the ACC Security Code. The guidance (attached to these comments) follows the basic steps of the NIST framework, is designed for users to design a cyber protection plan unique to the company or facility, and specifically implements the overall framework. The guidance is mapped directly to the frameworks' specific steps.

700 Second St., NE | Washington, DC 20002 | (202) 249.7000

Earlier in 2022, ACC approved a revised Security Code. The revised Code provides a platform for greater integration of site and cyber security programs within the chemical industry. Guidance for implementing the revised Security Code is currently being drafted.

ChemITC submits the following specific comments in response to the RFI for the NIST framework:

1. **Usefulness of the Framework**
   The framework provides a roadmap to establishing an organization's cyber risk profile. It can be used, often with other tools, as a benchmarking tool to assess cyber program effectiveness. This information is often used to help inform corporate management on the security capabilities and effectiveness of the cyber program.

2. **Benefits of Using the Framework**
   The framework provides a starting point to organizations of varying sizes and cyber capabilities. Chemical producers and users often combine the framework with standards such as ISO 27001. Combining the framework with such standards can help an organization determine its cyber protection maturity level.

3. **Challenges to Using the Framework**
   Since the framework was introduced in 2014, many organizations have noted that the framework's tiers do not represent cyber maturity levels. The framework could be improved by providing examples or information to users on how the framework matches up to maturity models. Additional training on the use of the framework may assist in expanding its implementation, especially among smaller organizations.

4. **Improvements to the Framework**
   The framework is an important guidance tool and is most useful by retaining its flexibility. Additional guidance or examples would be useful in helping organizations determine which tier their own risk management programs belong in. Also, consideration should be given to allow for continuous improvement within each tier.

5. **International Use of the Framework**
   ChemITC supports the adoption of the framework by other jurisdictions. NIST could further support the adoption of international documents that can be mapped to the framework.

6. **The Framework and Supply Chain Risk Management**
   Further integration of the framework with specific supply chain risk management standards may not be necessary. The voluntary, flexible approach of the framework should be retained. Prescriptive approaches for supply chain risk management should be

avoided. Providing examples of supply chain risk profiles and references to additional supply chain resources might be more helpful.

ACC looks forward to continuing working with NIST, DHS/CISA, and others in implementing the framework for the chemical sector. Please contact me at [redacted] with any questions regarding this submittal.

Sincerely,

Bill Gulledge

Bill Gulledge
Senior Director, Chemical Products & Technology Division
Manager, ChemITC Program