

From: **Gulledge, Bill**

Date: Mon, Apr 10, 2017 at 12:11 PM

Subject: Comments on the Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity

To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Please see attached comments. Thank you.

Bill

Bill Gulledge – Chemical Products and Technology Division

American Chemistry Council | 700 – 2nd Street NE | Washington, DC | 20002

www.americanchemistry.com

[Attachment Copied Below]

April 10, 2017

Via cyberframework@nist.gov

Mr. Edwin James
National Institute of Standards and Technology
100 Bureau Drive (Stop 8930)
Gaithersburg, MD 20899-8930

Re: ACC Comments- Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity

Dear Mr. James:

The American Chemistry Council's (ACC) Chemical Information Technology Center (ChemITC) submits the following comments regarding the chemical sector's experience with the Cybersecurity Framework¹. 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 joint industry-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 and consideration of metrics, generally represent enhancements to the original framework. We are also encouraged by the revised explanation of the relationship between implementation tiers and risk profiles.

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 the proposed enhancements to the framework are likely to encourage greater implementation across industry sectors and particularly within an industry supply chain.

Standards, guidance, and best practices relevant to cybersecurity are typically industry-driven and adopted on a voluntary basis; 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 provides this kind of helpful

¹ ACC represents the leading companies engaged in the business of chemistry. ACC members apply the science of chemistry to make innovative products and services that make people's lives better, healthier and safer. ACC is committed to improved environmental, health and safety performance through Responsible Care®, common sense advocacy designed to address major public policy issues, and health and environmental research and product testing. The business of chemistry is a \$770 billion enterprise and a key element of the nation's economy. Safety and security have always been primary concerns of ACC members, and they have intensified their efforts, working closely with government agencies to improve security and to defend against any threat to the nation's critical infrastructure.

global model to adopt. We encourage NIST to seek the engagement of critical sector stakeholders if the further development of metrics is planned. Any metrics should continue to be voluntary, developed by the framework users, and flexible enough to enable further innovation.

To augment existing programs within ACC, ChemITC prepared revised guidance (<https://chemitc.americanchemistry.com/RCSC-NIST-Framework-Guidance-Jan-2016.pdf>) to implement the cyber related activities under the ACC Security Code. The guidance, following the basic steps of the NIST framework, is designed for users to design a cyber protection plan unique to the company or facility, specifically implementing the overall framework. The guidance is mapped directly to the frameworks' specific steps.

ChemITC submits the following specific comments on the updated NIST framework:

1. Page 9, last paragraph- The relationship of target profiles and tier selection is an important one to recognize. Risk tolerance plays a role in selecting framework profiles regardless of tier selection.
2. Pages 10 – 12- The additions on supply chain risk management and integrated risk management programs are a welcome addition to the framework. The integrated risk management program description under Tier 4- Adaptive, is compatible with the risk-based approach used to implement cyber activities under the ACC Security Code. Also, the continuous monitoring of supply chain risk management policies, processes, and procedures reinforces one key goal of the framework: to implement more than just a one-time cyber risk management tool.
3. Page 15, Step 1 on Scoping- The additional explanation that implementation tiers may be used to convey risk tolerance is an important addition and again is compatible with the ChemITC cyber guidance.
4. Page 16, addition to Section 3.3 concerning implementation tiers- The addition of the last two sentences at the bottom of the page seems out of place and adds little value to the framework. The addition is a bit too global in scope.
5. Page 18, conclusion of Section 3.3- The example provided at the end of the section might be better placed in an appendix with more detailed description and additional examples like the brief ones provided in Section 4 on measurement.
6. Page 23- The distinction in Table 1 and the accompanying text between metrics and measures could be more clearly described. Again, illustrations in an appendix might be helpful. For example, how an integrated risk management program contributes to or is used as a metric could be described.
7. Page 24- The discussion on the application of metrics and measures seems to be more targeted to federal agencies and is very generic. Again, examples would be useful.

ACC looks forward to continue working with NIST, the DHS, and others in implementing the framework for the chemical sector. Please contact me with any questions regarding this submittal.

Sincerely,

Bill Gulledge

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