October 10, 2014

Via cyberframework@nist.gov

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive (Stop 8930)
Gaithersburg, MD 20899-8930

Re: ACC Comments- Experience with the Framework for Improving Critical Infrastructure Cyber Security

Dear Ms. Honeycutt:

The American Chemistry Council's (ACC) Chemical Information Technology Center (ChemITC) submits the following comments regarding experience with the Cybersecurity Framework. 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.

ChemITC supports the framework and its flexibility. The framework is complimentary to the Security Code included into ACC's Responsible Care® Program and other voluntary frameworks that have similar goals. The business of chemistry is global, and one goal of the NIST cyber framework is compatibility with frameworks used in other jurisdictions. In this regard, ChemITC continues to support Executive Order 13636, Improving Critical Infrastructure Cyber Security. The framework and the sharing of cyber threat information between government agencies and the private sector are important steps to implementing EO 13636.

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 would avoid burdening multinational enterprises with the requirements of multiple, and often conflicting, jurisdictions. We appreciate that NIST has been actively meeting with foreign governments to urge them to embrace the framework.

To augment existing programs within ACC, ChemITC is currently preparing a revision, based on the basic steps of the cyber framework, to supplement existing guidance to implement the cyber

related activities under the ACC Security Code. The guidance is being drafted for users to design a cyber protection plan unique to the company or facility, specifically implementing the overall framework. The revised guidance is scheduled to be completed by mid-2015.

To assist in the voluntary sharing of cyber threat information, ChemITC is also pilot testing an Information Sharing and Analysis Center (ISAC) to facilitate the dissemination of cyber threat data between DHS and other government agencies, and the chemical sector. The ISAC is scheduled to be fully operational by mid-2015. Sharing cyber threat information within the overall purpose of the framework would be incomplete without enacting information-sharing legislation that addresses or removes possible legal and regulatory penalties to allow for the quick exchange of data about evolving threats to our companies. ACC supports the passage of an information-sharing bill that contains protections related to lawsuits, public disclosure, regulations, and antitrust issues.

ACC looks forward to continue working with NIST, the DHS, and others in implementing the framework for the chemical sector. Please contact me at (202) 249-6714 or bill_gulledge@americanchemistry.com with any questions regarding this submittal.

Sincerely,

Bill Gulledge

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