April 8, 2013

Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899

RE: Request for Information, Federal Register Volume 78, Number 38 (Tuesday, February 26, 2013)

The American Chemistry Council (ACC) represents the leading companies engaged in the business of chemistry, a $760 billion enterprise and a key element of the nation's economy. ACC members apply the science of chemistry to make innovative products and services that make people's lives better, healthier and safer. It is one of the nation's largest exporters, accounting for twelve cents out of every dollar in U.S. exports. Chemistry companies are also among the largest investors in research development. Because of our critical role in the national economy and our responsibility to employees and communities—safety and security continue to be a top priority for members of the American Chemistry Council.

We are pleased to provide the following comments in response to your Request for Information (RFI) as published in the Federal Register Volume 78, Number 38 (Tuesday, February 26, 2013), pages 13024-13028. This RFI is part of a comprehensive review directed by the White House under Executive Order 13636 and implemented by the National Institute of Standards and Technology (NIST) in an effort to develop a framework to reduce cyber risks to critical infrastructure. The Framework will consist of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

The Framework will be developed through an open public review and comment process that will include workshops and other opportunities to provide input. The American Chemistry Council appreciates the opportunity to participate in this endeavor.

ACC agrees that NIST should engage critical infrastructure-appropriate stakeholders, including owners and operators, through a voluntary consensus-based process including interactive workshops along with other forms of outreach. The goal of this engagement is to identify cyber standards, guidelines and industry practices that will comprise the Framework. ACC believes that the Framework cannot be static, but rather must be a dynamic, living document that allows for ongoing consultation in order to address the ever evolving threats to critical infrastructure cybersecurity. A voluntary, consensus standards-based approach will facilitate the ability of critical infrastructure owners and operators to manage risk

and to help implement risk-based solutions from the bottom up with interoperability, scalability, and reliability.

Identification of Critical Chemical Infrastructure and Scope of Coverage

The identification of critical chemical infrastructure using a risk-based approach and defining the scope of coverage of the Cyber Security Framework are related issues that are critical for effective and efficient implementation. For example, the role of Government should include setting the example by including itself in the scope of coverage with the Framework. While there is a great interdependency within critical infrastructure, much of which is in the private sector, the private sector relies on government services. It seems that in any executive order, the compliance of Government to their own standards would be expected, if it is to have credibility in setting expectations with private industry.

Clear goals and objectives must be determined at the outset for each element comprising the framework. Overly simple or highly complex standards must be avoided. Cross-sector standards that require significant resources to comply with a "check-the-box" scheme can divert precious resources away from addressing the real threats in need of mitigation. Likewise, complex regulatory schemes can slow mitigation efforts. The first step in this process is to properly define critical chemical infrastructure.

In 2007, DHS issued the "Chemical Facilities Anti-terrorism Standards" (CFATS) regulatory program. This comprehensive federal regulatory program covers approximately 4500 facilities across the nation that possesses certain high hazard chemicals known as "Chemicals of Interest". Defined as a "high-risk chemical facility", each facility must register with DHS, conduct a comprehensive security assessment and implement protective measures that comply with 18 risk based performance standards (RBPS). Clearly defining the scope of coverage relating to application of the Framework is crucial to ensure that the proper level of attention and resources are applied where they are needed most. NIST should consider the CFATS definition of high risk chemical facility as a starting point in determining the scope of coverage for the chemical sector.

While CFATS may offer a good starting point, more work on defining what constitutes critical chemical facilities needs to be done. For example, one deficiency in the CFATS definition of "high-risk chemical facility" is that it doesn't address economic consequences or national security. From a cyber-critical perspective, potential impacts to the economy and national security are crucial factors that must be addressed when defining the scope of coverage for the Framework. Another issue with the CFATS definition is that it does not identify critical infrastructure. CFATS coverage includes any facility that stores or handles certain high hazard chemicals in sufficient quantities that could be used by a terrorist as a weapon, either via theft or diversion in commerce or by initiating an intentional release into the environment and surrounding community.

In 2001, ACC created a comprehensive security management system, the Responsible Care® Security Code, for which compliance is mandatory for members in ACC. The risk tiering system used by the Security Code for Tier 1 & 2 facilities would be appropriate for consideration in helping to identify critical chemical infrastructure. The Security Code defines Tier 1 & 2 based on risk factors unique to the facility including the types and quantities of hazardous chemicals stored and handled at the facility, the potential severity of consequences to the economy and the surrounding population as a result of a successful attack and the difficulty of attack based on the level of coordination and number of individuals required and their level of training. In addition, the Responsible Care Program has international recognition and is applied globally across the chemical sector by international organizations such as the International Council of Chemical Associations (ICCA) (http://www.icca-chem.org). Through the participation of over 50 national chemical manufacturing associations, Responsible Care forms an essential part of ICCA's contribution to the United Nations' Strategic Approach to International Chemicals Management (SAICM).Given the borderless, global nature of the cyber security threat, leveraging an internationally recognized approach is appropriate.

Cyber Security Threat Information Sharing

While the development of the Framework is an important part of a comprehensive strategy to protect critical infrastructure against international cyber security threats, the foundation of the strategy must be an effective process for two-way sharing of threat information that is timely, specific and actionable. We commend the attention given to the important topic in the Executive Order and on Capitol Hill in such legislative proposals such as the Cyber Information Sharing and Protection Act (CISPA), sponsored by Representative Mike Rogers in the House and the Secure IT Act sponsored by John McCain in the Senate and offered in the last Congress. Although these bills were not enacted into law, they offered a sound approach for an improved information sharing process. The varying legislative proposals contained provisions that could greatly enhance the ability for owners and operators of critical infrastructure to apply risk management standards, guidelines and industry practices in a targeted way that will have a maximum impact on identifying and implementing protective solutions. Key elements of an effective threat information sharing process must include:

- Declassification of threat information, where possible, to ensure maximum coverage.
- Increased issuance of security clearances to owners and operators of critical infrastructure who operate on the front lines to combat cyber threats.
- Improved sharing of threat and incident information internal to Federal, State and local law enforcement, homeland security and intelligence organizations as well as the sharing of such information with and between the owners and operators of critical infrastructure.
- Incentives for the private sector that would encourage the sharing of threat and incident information within the owner/operator community as well as within the Federal Government.
- Information Protections that would prevent disclosure of such information to the public.

A formal government- administered program to classify information and provide protection from subpoena in civil litigation or disclosure under the Freedom of Information Act (FOIA) is essential if organizations are expected to share and report sensitive and/or proprietary information. The DHS Chemical -terrorism Vulnerability Information (CVI) Program under CFATS or the DOT Security Sensitive Information (SSI) Program could serve as a model for such programs.

Information Technology and Telecommunication Services:

For any cyber security strategy to be truly effective, it is crucial that all parties in the supply chain share the responsibility of providing an effective defense against the global cyber threat. The chemical sector commonly uses a layer of protection strategy for both physical and cyber security that relies on a multi-pronged strategy covering prevention, protection and mitigation measures. While we agree that owners and operators of critical infrastructure play a critical role in protecting their systems, processes and information, the IT and telecommunication sectors play an equally critical role to ensure that software and hardware products and telecommunication services are provided to the end user community that have the most up to date and advanced cyber security protection available. In particular, Telecommunication Services, Government Networks and Critical Infrastructure, all rely on the IT Software, Service and Hardware suppliers. Therefore, the IT industry has a higher stewardship responsibility to work with all critical infrastructures to ensure their products are secure for their intended use. Telecommunication service providers offer the best opportunity to identify cyber intrusions at the root of the issue and to protect critical infrastructure systems and end users that are located further downstream.

Risk Management

Generally, the Chemical Sector employs international standards such as ISO/IEC 27001 and IEC 62443 as the framework for the IT security risk assessment process. Depending on the subject of the assessment, the assessment tool is tuned to evaluate compliance with a company's specific security standards, policies and other control objectives. Risks are categorized leveraging a standard scoring process to define risks based on likelihood and impact, within the context of risks to confidentiality, integrity, availability. The risk assessment activity is incorporated into a project methodology**.**

Chemical Industry Cyber Security Practices

Chemical sector companies practice cyber security through a combination of voluntary, sector driven and regulatory practices, as described in the following paragraphs.

ACC Responsible Care Security Code:

To date, ACC members have invested nearly $11 billion to bolster security at its manufacturing sites and across the global supply chain through Security Code implementation. In addition to the opportunity to leverage the Tiering definitions for defining critical chemical infrastructure, the Security Code is the gold standard for the industry and has served as a model for numerous federal, state and local regulatory

programs. The Security Code specifically calls on ACC members to:

- Assess cybersecurity vulnerabilities and dedicate resources to address them
- Provide appropriate training and guidance to employees on cybersecurity threats
- Conduct periodic drills or exercises to test cybersecurity systems
- Work with designated authorities to share information from cybersecurity incidents
- Periodically audit cybersecurity systems to identify opportunities for improvement

Responsible Care compliance is an obligation for membership into the ACC. Responsible Care Members are audited every three years by a third-party, certified independent auditor. If found in non-compliance, a company's ACC membership can be terminated.

Federal Regulations:

In 2007, DHS issued the "Chemical Facilities Anti-terrorism Standards" (CFATS) regulatory program. This comprehensive federal regulatory program covers more than 4500 high-risk chemical facilities across the nation that possesses certain high hazard chemicals known as "Chemicals of Interest". Each high-risk chemical facility must register with DHS, conduct a comprehensive security assessment and implement protective measures that comply with 18 risk based performance standards (RBPS). RBPS #8 specifically addresses cyber security performance standards designed to deter cyber sabotage and prevent unauthorized access to critical chemical process control systems.

CFATS identifies "critical cyber systems" that require enhanced security measures. Critical systems are defined as those which:

- Monitor or control physical processes that contain a chemical of interest (COI);
- Are connected to other systems that manage physical processes that contain a COI;
- Contain sensitive business information or personal information that, if exploited, could result in theft, diversion or sabotage of a COI.

CFATS requires a combination of policies and practices designed to effectively secure cyber systems from attack or manipulation. Key cyber elements inspected for compliance include:

- General IT policies. (Password management, administrative controls, access control and asset disposal policies)
- Ordering systems and Data Center. (Segregation of duties and administrative rights)
- Network segmentation. (How networks are segmented from corporate networks)
- Network Configuration. (Review of detailed network diagrams and wiring drawings. LAN diagrams for the plant and wiring for process control equipment)
- Plant automation control/computer systems. (System updates, virus protection and upgrade strategies)

Covered CFATS facilities are inspected for compliance by DHS and can be shut down or fined if found to be non-compliant.

Voluntary Industry Standards for Cyber Security:
The Chemical Sector generally applies a comprehensive set of policies, standards and procedures based on guidance from organizations such as the National Institute of Standards and Technology (NIST), the International Society for Automation (ISA), the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Primary industry standards in this space include ISO 27001 and ISA/IEC- 62443.

Published in October 2005, ISO/IEC 27001 is part of the growing 27000 family of standards covering information security management systems (ISMS). Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements. ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

ISA/IEC-62443 is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). This guidance applies to end-users (i.e. asset owner), system integrators, security practitioners, and control systems manufacturers responsible for manufacturing, designing, implementing, or managing industrial automation and control systems.

The majority of the ISA/IEC 62443 standards are developed by the ISA99 committee of the International Society for Automation (ISA). The committee's focus is to improve the confidentiality, integrity, and availability of components or systems used for manufacturing or control and to provide criteria for procuring and implementing secure control systems. Compliance with the Committee's guidance will improve industrial control system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing industrial control systems degradation or failure. As each standard is developed, it is submitted simultaneously to ANSI and IEC as a U.S national and international standard, respectively.

Cyber Security Partnerships and the Chemical Sector

As cyber threats continue to evolve, the chemical industry is proactively working with DHS and others dedicated to improve threat information sharing between the public and private sectors and by enhancing the security of industrial control and business systems through the sharing of industry practices to enhance preparedness and response to cyber threats. Therefore, ACC, in collaboration with the Chemical Sector Coordinating Council launched the “Roadmap Implementation Website” (www.chemicalcybersecurity.com). The Roadmap Website serves as a clearing house for information

and provides a dashboard on progress for securing process control systems in the chemical sector. Other partnerships within the chemical sector include:

- **ChemITC:** Chemical Information Technology Center (ChemITC®) of the American Chemistry Council (ACC) is a forum for companies in and associated with the ACC to address common IT issues. Through strategic programs and networking groups dedicated to addressing specific technology issues, ChemITC® is committed to advancing the cyber security of its member organizations.

- **Chemical Sector Coordinating Council (CSCC):** Pursuant to the Homeland Security Act of 2002, the purpose of the CSCC is to facilitate effective coordination and collaboration between federal infrastructure protection programs, the infrastructure protection activities of the private sector and those of state, local, territorial and tribal governments.

- **National Infrastructure Advisory Council (NIAC):** The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructures, both physical and cyber, supporting sectors of the economy.

- **International Society for Automation (ISA):** ISA has primary responsibility for the development of the ISA-62443 series of standards addressing cyber security for industrial automation and control systems (IACS). As each standard is developed it is submitted simultaneously to ANSI and IEC as a U.S. national and international standard, respectively.

- **Industrial Control Systems Joint Working Group (ICSJWG):** The Department of Homeland Security (DHS) established the Industrial Control Systems Joint Working Group (ICSJWG) to facilitate information sharing and reduce risk to the nation's industrial control systems. The ICSJWG provides a vehicle for communicating and partnering across all critical infrastructure sectors between federal agencies and departments, as well as private asset owners and operators of industrial control systems. The goal of the ICSJWG is to enhance the collaborative efforts of the industrial control systems community by accelerating the design, development, and deployment of secure systems.

- **InfraGard:** InfraGard is a Federal Bureau of Investigation (FBI) program that was initiated in 1996. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. InfraGard is a partnership between the FBI and the private sector including individuals, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. FBI works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C. and with the DHS in support of its Critical Infrastructure Protection mission.

- **Partnership for Critical Infrastructure Security (PCIS):** As the principal cross-sector advisory group to the US Government, the PCIS works with the individual trades, the sector specific agencies (SSAs) and the Sector Coordinating Councils (SCCs) to provide advice and counsel on issues that have a

broad impact on the nation's critical infrastructure, and the owners and operators responsible for system security

Thank you for this opportunity for members of The American Chemistry Council to provide comments on this critical issue. If you have any specific questions, or require more information, please feel free to contact me at your convenience.

Sincerely,
William Erny
Senior Director
American Chemistry Council
700 2nd Street N.E.
Washington, DC 20002
202-249-6412
Cell: 703 200 7044