Daniel J. Strachan
Director
Industrial Relations &
Programs

**American
Fuel & Petrochemical
Manufacturers**

1667 K Street, NW
Suite 700
Washington, DC
20006

202.457.0480 office
202.552.8475 direct
202.457.0486 fax
Dstrachan@afpm.org

February 9, 2016

**Docket Number 151103999-5999-01
National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899-8930
Attn: Diane Honeycutt**

RE: AFPM Comments on "Views on the Framework for Improving Critical Infrastructure Cybersecurity"

AFPM, the American Fuel & Petrochemical Manufacturers[1], appreciates the opportunity to provide comments on the "Views on the Framework for Improving Critical Infrastructure Cybersecurity" Request for Information (80 FR 76934, December 11, 2015). Since many AFPM member sites have both industrial control systems (ICS) and enterprise systems (IT), therefore we have considerable interest in the Framework for Improving Critical Infrastructure Cybersecurity ("Framework").

The Framework was designed to provide guidance to facilities deemed to be part of the Critical Infrastructure as defined by Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." The Framework relies on existing standards and best practices to achieve outcomes that can assist organizations in managing their cybersecurity risk. The Framework was designed to be evergreen, evolving with technological and business advances.

I. <u>General Comments</u>

Many AFPM members have cybersecurity standards, methodologies and procedures already in place at their facilities. AFPM members added the Framework as an additional tool that they can employ in keeping their systems secure. AFPM members believe that a benefit of the Framework is that it provides a sample of what a company can implement and it succinctly describes what is necessary in the foundation of a good cybersecurity risk program.

[1] AFPM, the American Fuel & Petrochemical Manufacturers is a trade association representing high-tech American manufacturers of virtually the entire U.S. supply of gasoline, diesel, jet fuel, other fuels and home heating oil, as well as the petrochemicals used as building blocks for thousands of vital products in daily life. AFPM members make modern life possible and keep America moving and growing as they meet the needs of our nation and local communities, strengthen economic and national security, and support 2 million American jobs.

AFPM also believes that in today's critical infrastructure, physical and cybersecurity measures necessarily overlap. The Framework could be improved by implementing the role of physical security in any discussion of cybersecurity.

II. The Framework Must Remain Voluntary

As stated in our original comments submitted on December 13, 2013, AFPM believes that in order for the Framework to be most effective in critical infrastructure, it must remain voluntary. Having the Framework remain voluntary is vital to its acceptance and use in critical infrastructure. Some of the measures referenced in the Framework are not appropriate at all facilities. In addition, the Framework should clarify that the Informative References are not mandatory.

A Framework that is mandated through regulation or legislation will not benefit private industry. As an example, AFPM members presently use the Framework along with other tools to ensure secure systems. If the Framework were to become mandatory, AFPM members might be unable to effectively use portions of the Framework as they may conflict with existing industry practices. Further, due to the fact that an update to a compulsory document would have to go through many time-consuming steps to be approved, it not be able to keep up with changing technologies. The result would be that the original intent of the Framework would be lost and it would simply become a static and ineffective checklist.

III. Integration of Cybersecurity Risk Management into Business Risk Management

As stated in AFPM's 2013 comments, the Framework needs to place more emphasis on Industrial Control Systems ("ICS"). While ICS are referenced within the Framework, the Framework is more oriented toward enterprise systems.

In addition, the Framework needs to address the entire supply chain, not only the asset owners. Regardless of sector, asset owners are dependent upon the supply chain in their sector or in other sectors. A cybersecurity disruption to the supply chain could prove disastrous to asset owners. An example of this would be a cyber-attack on the financial sector. Disruptions in the financial sector caused by cyber-attacks could in turn negatively affect the purchase of crude oil that is used in refineries. The end result could cripple the flow of feedstocks necessary to produce fuels or other products in refineries. The Framework does recognize the interdependencies of many of the critical infrastructures and this should be the basis for additions to the Framework with regard to supply chain issues.

IV. Additional Comments

AFPM provides the following additional comments:

- NIST should use the recent passage of the Cybersecurity Information Sharing Act of 2015 to foster sharing of best practices across companies and industries. The various Information Sharing and Analysis Centers ("ISAC") are well-suited to share information on best practices.

- AFPM believes that NIST should continue to be the sole organization responsible for the development of the Framework. We believe that NIST has done a very good job in coordinating Framework issues and it is the best, and most logical, organization to continue this task.

- The Framework should not duplicate nor conflict with existing regulatory programs such as the Chemical Facility Anti-Terrorism Standards ("CFATS") or the North American Electric Reliability Corporation ("NERC") cybersecurity standards program.

- Finally, AFPM believes that "objectives" would be a better word choice than "outcomes" in the document. Utilizing the word "objectives" would align the framework with the Control Objectives for IT ("COBIT") and ISO/IEC 27001 "Information Technology – Security Techniques – Information Security Management Systems – Requirements." Both of which are utilized commonly in enterprise systems in critical infrastructures.

AFPM looks forward to continuing an open, constructive dialogue with NIST on the improvement of the Framework. If you have any questions, or if AFPM can be of any assistance, please contact me at (202) 552-8475 or at dstrachan@npra.org

Sincerely,

DJ Strachan

Daniel J. Strachan
Director, Industrial Relations & Programs