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

December 13, 2013

Docket Number 130909789-3789-01
National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Stop 8930
Gaithersburg, MD 20899-8930
Attn: Adam Sedgewick

RE: AFPM Comments on "Preliminary Cybersecurity Framework"

AFPM, the American Fuel & Petrochemical Manufacturers, appreciates the opportunity to provide comments on the "Preliminary Cybersecurity Framework" Notice and Request for Comments (78 FR 6448, October 29, 2013). Many AFPM member sites have both industrial control systems (ICS) and enterprise systems (IT), therefore we have considerable interest in the development of the Preliminary Cybersecurity Framework ("Framework").

The Framework is 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 will be evergreen evolving with technological and business advances.

I. General Comments

AFPM staff and member companies have been involved in the development of the Framework throughout 2013, including attending all Framework workshops sponsored by the National Institute of Standards and Technology ("NIST"). We applaud NIST for its role in promoting industry-led, global cybersecurity standards and best practices developed by public-private standards development organizations.

AFPM understands that the Framework would cover all critical infrastructure sectors as determined by the Department of Homeland Security ("DHS"). To that end, the Framework is broad in scope. While this broad scope makes the Framework useful to a variety of sectors, NIST must recognize that this same breadth could lead to misinterpretation or misapplication. It will be the responsibility of NIST to ensure that the recommendations of this framework are applied appropriately to all stakeholders

Many AFPM members have cybersecurity standards, methodologies and procedures already in place at their facilities. AFPM members plan to use the Framework as an additional tool that they can utilize to keep their systems secure. AFPM members state that a benefit of the Framework is that it is a sample of what a company can implement and it describes what is necessary in order to have the basics of a good cybersecurity risk program.

AFPM also believes that in today's critical infrastructure, physical and cybersecurity measures necessarily overlap. The Framework needs to consider the role of physical security in any discussion of cybersecurity.

II. Voluntary Adoption of Framework

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 in critical infrastructure. The Framework should state that its adoption is a broad menu of options and that businesses do not need to undertake all the cybersecurity activities listed in the Framework Core. Indeed, some of the measures referenced in the Framework would not be appropriate at all facilities. The Framework should clarify that the Informative References are neither exhaustive nor mandatory.

A Framework that is mandated through regulation or legislation will not benefit private industry. As stated above, AFPM members will use the Framework along with other tools to ensure secure systems. If the Framework were to become a mandated regulation, AFPM members would not be able to utilize the Framework as the useful tool that it is intended to be, as they might have to implement portions of the Framework which may conflict with existing industry practices

III. Integration of Cybersecurity Risk Management into Business Risk Management

AFPM's review of the Framework shows that it would likely be tested and adopted by entities that have function enterprise risk management programs. 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 solely 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. This would disrupt the purchase of crude oil that is used in refineries. The Framework does recognize the interdependencies of many of the critical infrastructures and this should be the basis for growth of the Framework in address supply chain issues.

IV. Additional Comments

The Framework should not duplicate or 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.

AFPM noticed that throughout the framework, the word "outcomes" is used quite often. AFPM believes that "objectives" would be a better word choice, as this 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.

With regard to privacy and civil liberties, AFPM believes that privacy-protection assessments should be weighed only in the context of the voluntary adoption of the framework by entities in a critical infrastructure sector. AFPM reminds NIST that the fundamental objective of the Framework is to reduce cybersecurity risks that critical infrastructure entities face. Further, AFPM strongly urges the administration to make clear in the Framework that privacy protections are being contemplated solely in the context of critical infrastructure cybersecurity activities.

Finally, AFPM believes that the Framework would be incomplete without the enactment of information-sharing legislation that is supported by the business community, and we welcome working with the administration and Congress toward this goal.

AFPM looks forward to continuing an open, constructive dialogue with NIST on the development 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,

Daniel J. Strachan
Director, Industrial Relations & Programs