From: **Dan Strachan**
Date: Fri, Apr 7, 2017 at 11:02 AM
Subject: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

Attached, please find comments on the above subject from American Fuel & Petrochemical Manufacturers.

Please let me know if you have any questions.

Regards,

Daniel J. Strachan
Director
Industrial Relations & Programs

American
Fuel & Petrochemical
Manufacturers
1667 K Street NW
Suite 700
Washington, DC 20006

Dstrachan@afpm.org
Learn more about AFPM at afpm.org

[Attachment Copied Below]

April 10, 2017

Department of Commerce
National Institute of Standards and Technology
100 Bureau Drive
Stop 8930
Gaithersburg, Maryland 20899
Attn: Edwin Games

RE: "Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity"

AFPM, the American Fuel & Petrochemical Manufacturers[1], appreciates the opportunity to comment on the Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity."[2] Many AFPM member sites have both industrial control systems (ICS) and enterprise systems (IT), and have a significant interest in the current and future states of cybersecurity.

AFPM members span both the energy and chemical industries – two industries where the state of cybersecurity is of the utmost concern. Based on their collective expertise regarding best practices, AFPM's members believe that a document such as the Framework for Improving Infrastructure Cybersecurity ("the Framework") should be revised on an ongoing basis to remain relevant to the public and private sectors. The Framework provides AFPM members with voluntary guidance, utilizing existing standards, guidelines and practices to better measure a facility's cybersecurity risk management

AFPM member companies utilize the Framework as one of the many cybersecurity risk management tools at their disposal. In addition, AFPM members also use other risk management and analysis tools, including the DOE Cybersecurity Maturity Model ("C2M2") and third-party assessments. These tools enable AFPM's members to assess the status of their risk management and highlight areas for improvement. It is imperative that these documents are constantly revised to keep up with technology advances to remain beneficial.

I. Updates in Version 1.1

NIST listed four major updates in Version 1.1.

---

[1] AFPM is a trade association whose members include nearly 400 companies that encompass virtually all U.S. refining and petrochemical manufacturing capacity.
[2] 82 Federal Register 8408 (January 25, 2017).

The first update is the addition of Section 4.0, "Measuring and Demonstrating Cybersecurity." AFPM agrees with this addition as it takes the Framework and makes it applicable to business objectives through various matrices and measurements, as shown in the table in paragraph 4.2. Many users of the Framework have already developed measurement systems incorporating the Framework at their facilities. The addition of Section 4.0 to the updated Framework, allows users to easily apply the Framework to their current risk management strategies.

The second update is the expanded explanation of using the Framework for cyber supply chain risk management (SCRM) purposes. AFPM applauds this expanded explanation as it further clarifies the paramount importance of cybersecurity in supply chain management. As with many other critical infrastructures, fuel and petrochemical manufacturers are dependent on the supply chain to continue the production and distribution of their products. We agree with the intentions of the National Institute of Standards and Technology (NIST) to have stakeholders better understand cyber SCRM and support the addition of the new category Supply Chain Risk Management (ID.SC) to the Framework.

The third update includes refinements to better account for authentication, authorization and identity proofing. AFPM agrees that this area of the Framework needed clarification. AFPM supports the addition of the Subcategory PR.AC-6 with its informative references to the Framework.

The fourth update is a more detailed explanation of the relationship between Implementation Tiers and Profiles. AFPM sees this as further clarifying the use of the various tiers in the Framework. AFPM believes that this clarification will enable more stakeholders to utilize the Framework.

II. Conclusion

AFPM members were involved in the development of the original framework and have utilized the Framework as a risk management tool in many of their facilities. Much like a standard, the Framework must be updated periodically if it is to remain dynamic and useful.

AFPM believes that the Framework is most effective in critical infrastructure as a voluntary measure. The Framework should state that its approach will remain 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 continue to clarify that the Informative References are neither exhaustive nor mandatory.

A Framework that is mandated through regulation or legislation will not benefit or be supported by private industry. As stated above, AFPM members 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

AFPM looks forward to continuing an open, constructive dialogue with NIST on the continuing development of the Framework. If you have any questions or if AFPM can be of any assistance, please contact me.

Sincerely,

Daniel J. Strachan
Director, Industrial Relations & Programs