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

September 9, 2016

National Institute of Standards and Technology
100 Bureau Drive
Stop 2000
Gaithersburg, Maryland 20899
Attn.: Nakia Grayson

RE: "Information on Current and Future States of Cybersecurity in the Digital Economy" – Docket No. 160725650-6650-01

AFPM, the American Fuel & Petrochemical Manufacturers[1], appreciates the opportunity to comment on the Request for Information (RFI) entitled "Information on Current and Future States of Cybersecurity in the Digital Economy." (81 Fed. Reg. 52827) Because many AFPM member sites have both industrial control systems (ICS) and enterprise systems (IT), our members have a significant interest in the current and future states of cybersecurity.

The Commission on Enhancing National Cybersecurity ("Commission") plays an important role in determining the future of cybersecurity, serving as a conduit for constructive ideas from both the public and private sectors. The Commission can be an advocate for sensible governmental policies that serve to protect industries as they report incidents and share other cybersecurity information.

Many 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 information sharing, collaborative efforts between critical infrastructure operators, and technical innovations from the private sector are crucial aspects of effective cybersecurity policy, and the Commission's recommendations should reflect those priorities.

I. Current Trends and Challenges

Information sharing, risk management tools, and cybersecurity investments are the most significant current trends in critical infrastructure cybersecurity. With the passage of the Cybersecurity Information Sharing Act of 2015, many obstacles to sharing information and reporting incidents were ameliorated. Information Sharing and Analysis Organizations ("ISAOs") and Information Sharing and

[1] AFPM is a trade association whose members include nearly 400 companies that encompass virtually all U.S. refining and petrochemical manufacturing capacity.

Analysis Centers ("ISACs") have been established solely for the exchange of information and incident reporting across industries, academia, regional governments and other entities. AFPM's members are involved in these organizations and utilize them for timely information sharing. The Commission should work closely with ISACs and ISAOs to obtain timely information and avoid duplicative reporting

AFPM's members also use many risk management and analysis tools, including the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, the DHS Critical Infrastructure Cyber Committee ("C^{3}"), and third-party assessments. These tools enable AFPM's members to assess the status of their risk management and highlight areas for improvement. It isimperative that these documents are revised as technology advances to remain beneficial.

The main challenge that AFPM's members face with regard to government's role in cybersecurity is the lack of coordination between government agencies. Depending on the facility, an AFPM member may have to consider criteria from the Department of Energy, the Department of Homeland Security, the US Coast Guard, as well as state entities such as the National Guard. This patchwork of potentially conflicting requirements is inefficient, can cause confusion, and can lead to misinformation or misinterpretation of a policy or recommendation. AFPM strongly urges the Commission to improve coordination between government agencies with regard to cybersecurity.

Another challenge faced by private industry is information overload. It is common for an AFPM member to receive dozens of emails per day regarding cybersecurity. Some of these emails are from other private entities, but many are from government agencies, including the several Departments mentioned above. Further, AFPM's members have expressed concern that alerts on cyber incidents are not highlighted in the agencies' emails, which could cause a company to overlook the alerts. Alerts on cyber incidents must be brought to the forefront in any communication as it is critical that the information is conveyed to industry in a timely and prominent manner.

II. Future Trends and Challenges

In addition to current trends and challenges, AFPM anticipates three future trends with respect to cybersecurity: (1) increased incident reporting and information sharing including sharing across interdependent sectors; (2) continuing collaboration and coordination between the information technology/enterprise systems, industrial control systems, and physical security areas of facilities; and (3) an increase in cybersecurity awareness across the entire supply chain.

AFPM has also identified four future challenges: (1) the development of new technologies; (2) an increase in attacks directed at industrial control systems; (3) the potential growth of ransomware; and (4) the potential for increased regulation following a cybersecurity incident.

The pace of technological advances is ever increasing, and with each new technical innovation comes an increasing need for timely cybersecurity tools and education, which should be routinely reviewed to ensure that they are current, given the present state of technology.

While industrial control systems have been targeted by cybersecurity attacks before, the 2015 attack on the Ukraine power grid showed many the consequences of a successful attack on an industrial control system in a critical infrastructure. The success of that attack and the corresponding worldwide media coverage could persuade others to attempt similar attacks on industrial control systems.

Currently, ransomware does not pose as much of a threat as other cybersecurity issues. However, the scope and deployment of ransomware is growing quickly and must be kept in check, given the anticipated sophistication of such software

If there is a demonstrated need for increased regulation following a cybersecurity incident, AFPM believes that both public and private entities must work together to develop sensible regulation. We would oppose prescriptive regulation developed in haste without private sector stakeholder input as that would sully the cooperative relationship that has developed between the public and private sector stakeholders.

III. Progress to Address the Challenges

AFPM has seen considerable progress made to date with respect to some of the challenges outlined above. For example, in 2015, the U.S. Coast Guard (USCG) started a bulk liquid transfer operations project. The USCG collaborated with NIST, using the NIST Cybersecurity Framework as a guide for the project. USCG has also recently begun a dialogue with the Defense Logistics Agency (DLA) as they work on a similar project.

In order to expand information sharing on important topics, AFPM strongly supports the efforts of the Department of Homeland Security (DHS) to review classified information to evaluate whether the information should remain classified or if it can be released to a larger audience. AFPM understands the need to keep certain information secure but also recognizes that sharing relevant and timely information is paramount to deter cybersecurity attacks.

Lastly, AFPM has noticed that communication between the public and private sectors has improved in 2016, which has strengthened working relationships and benefited all who are involved. This improved working relationship should assist us in seeking effective solutions following any harmful cybersecurity incident.

AFPM believes that information sharing is the most promising approach to addressing the challenges listed above. Whether cybersecurity information sharing or incident sharing, the exchange of

information will be beneficial to all parties involved. However, as discussed above, all parties involved should aim to share only useful and actionable information to avoid information overload.

IV. Short and Long Term Recommendations

AFPM's members offer several ideas that could be implemented in the short term to address these challenges:

- First, and most importantly, the Commission should strive to ensure that government agencies do not engage in redundant projects or implement duplicative policies with regard to cybersecurity. Doing so will eliminate inefficiencies and save resources.
- The Commission should work with agencies that handle classified information on cybersecurity to investigate if more of what is currently considered "classified" can be released as unclassified information.
- The Commission should explore a way to streamline the reporting and compliance procedures for the private sector. This would allow entities in the private sector to report an incident without taking away critical time to mitigate the incident.
- The Commission should also educate smaller businesses on the importance of cybersecurity. Many small businesses sell to AFPM's members, and there is concern that harmful entities could use the small businesses' lack of adequate cyber defenses as conduits to larger systems.
- Finally, AFPM asks the Commission to keep the NIST Cybersecurity Framework as a voluntary tool and not allow it to be used for political purposes. AFPM believes that NIST should continue to be the sole organization responsible for the development of the Framework. We believe that NIST has done an excellent job in coordinating Framework issues and is the best and most logical organization to continue this task.

In the long term, AFPM is most concerned about the possibility of international cyber-attacks. As many cyber-attacks originate overseas, AFPM would like to see more international treaties that contain language stating that a hacker could be extradited to the country affected by their actions to stand trial.

As technology evolves, the balance between security and convenience will become increasingly more acute for average citizens and businesses. The public and private sectors must always assure that cybersecurity is never compromised in the pursuit of convenience.

AFPM's members know that cybersecurity attacks will continue and will likely grow in complexity. Therefore, we ask that the Commission champion the effort for private and public entities to work together as a team to stay ahead of the hackers. AFPM believes that this teamwork will reap benefits for years to come.

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

Sincerely,

Daniel J. Strachan
Director, Industrial Relations & Programs