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

April 29, 2013

Docket Number 130206115-3115-01
Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, N.W. Room 4725
Washington, DC 20230
Attn: Alfred Lee

RE: AFPM Comments on "Incentives to Adopt Improved Cybersecurity Practices"

AFPM, the American Fuel and Petrochemical Manufacturers, appreciates the opportunity to provide comments on the "Incentives to Adopt Improved Cybersecurity Practices" Notice of Inquiry (NOI) (78 FR 18954, March 28, 2013). Many AFPM member sites have both industrial control systems (ICS) and enterprise systems (IT) ; therefore we have considerable interest in the development of a set of incentives that would affect the refining and petrochemical industries.

I. General Comments

AFPM appreciates the opportunity to provide comment during the early stages of development of the incentives. Requesting information from industry prior to rulemaking will provide real value to the Department of Commerce.

President Obama's Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" ("Executive Order") emphasized that the National Institute of Standards and Technology (NIST) is to incorporate in the Cybersecurity Framework "industry best practices" as well as voluntary consensus standards, "to the fullest extent possible." The development of incentives is necessary to promote participation in this framework.

II. Questions Posed in the NOI

In the NOI, Commerce posed a number of questions. While AFPM does not answer all the questions, it does provide feedback on a number of questions included in the NOI.

- Are existing incentives adequate to address the current risk environment for your sector/company?

Presently, there are no specific government-sponsored incentives. Current incentives are self directed by the sector to maintain business processes, supply chains, continuity and industrial processes. This may have an impact on other compliance and regulatory requirements, for example Sarbanes-Oxley. AFPM members also rely on risk assessments to help determine the proper level of mitigation to apply.

- Do particular business sectors or company types lack sufficient incentives to make cybersecurity investments more than others? If so, why?

The scope of our response is limited to petroleum refineries and petrochemical manufacturing facilities. AFPM members operate multi-billion dollar facilities and are extremely motivated to protect their companies, even without government incentives.

- How do businesses/your business assess the costs and benefits of enhancing their cybersecurity?

Assessment is done on the basis of risk versus reward scenarios, the higher the risk, the more mitigation is applied.

- What are the best ways to encourage businesses to make investments in cybersecurity that are appropriate for the risks that they face?

Drive an industry risk-based approach, which fulfills an achievable baseline objective for critical infrastructure, augmented with industry-developed specifications on architecture, network devices and configurations. Drive the identification of critical nodes, single points of failure and/or interfaces to industrial control systems (SCADA etc), then review these assets/interfaces from known and likely cyber threat vectors. Ensure that these incentives help companies address the real risks, as opposed to meeting arbitrary requirements.

- How do businesses measure success and the cost-effectiveness of their current cybersecurity programs?

This can vary by company, but many AFPM members use internal metrics to measure mitigation of risks. Abroad generic "audit policy" would not be applicable due to the differences from facility to facility.

- Are there disincentives or barriers that inhibit cybersecurity investments by firms?

Yes, if the cost to implement and maintain security exceeds the business benefit derived over the lifecycle of the business deliverable.

- Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively?

With respect to multi-national corporations, different countries and regions may not allow security controls such as encryption and secure connections, this may require segmenting and securing the network architecture effectively globally within a multinational company.

- If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?

A concern is the high cost to comply with 'forced audits' or 'check-box' audits. Small businesses have a difficult time knowing what to do, since they usually have smaller IT departments, so having a good, easy-to-follow high-level framework, with examples that would apply to companies of various sizes, is beneficial.

Multinational companies need to assess the barriers, disincentives and challenges both globally and regionally, and draft a best practices model/framework on how to best to reduce the cybersecurity exposures to doing business regardless of location.

- Are incentives different for small businesses? If so, how?

While the scope is less and limited to a local region, the mitigation of risks is still the same regardless of the size of the facility. AFPM members are large businesses and have the benefit of employing security professionals who have knowledge of current cybersecurity risks and mitigations.

- For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?

The costs vary by facility, but it can be burdensome. Costs associated with compliance will be considered as part of the decision to pursue a business activity. It will take into account the potential costs of an incident, and the total cost of implementation and maintenance of the enhanced security.

- What are the merits of providing legal safe-harbors to individuals and commercial entities that participate in the DHS Program?

This may be an essential incentive to promote enhanced security, as individuals and commercial entities transition to securing their networks under a DHS program.

- By contrast, what would be the merits or implications of incentives that hold entities accountable for failure to exercise reasonable care that results in a loss due to inadequate security measures?

Information risks are ubiquitous and involve not only technical controls but individual behavior that may circumvent even the best configured secured network. Reasonable care is a good benchmark, but may require a more robust and transparent definition as to what reasonable means.

- How can liability structures and insurance, respectively, be used as incentives?

Liability structures are a basically a risk scenario, whereby the downside of non-compliance is met with fines and penalties, which would make it impractical for companies to ignore. An insurance incentive would reduce claims by businesses who effectively comply with a DHS program –serving to achieve compliance by reward, such as government financial incentives and or grants.

- What other market tools are available to encourage cybersecurity best practices?

An International Standards Organization (ISO) compliance certification is an example of a tool that can address network security, as well as SANS, CISCO and other certifications.

- Should efforts be taken to better promote and/or support the adoption of the Framework or specific standards, practices, and guidelines beyond the DHS Program? If so, what efforts would be effective?

AFPM supports promoting, but not requiring, the adoption of a particular framework, standard practices and guidelines and notes that these alternatives may exceed the requirements contemplated under the DHS program.

- In what way should these standards, practices, and guidelines be promoted to small businesses and multinationals, respectively, and through what mechanisms? How can they be promoted and adapted for multinational companies in various jurisdictions?

As every facility is different in size and requirements, it becomes a matter of scale. AFPM believes that referral to specific fit-for-purpose standards, practices, and guidelines for each respective entity would be helpful. A company could determine which would be the best models for their various facilities both domestic and international.

- What incentives are there to ensure that best practices and standards, once adopted, are updated in the light of changing threats and new business models?

The key to incentivizing response to change is for the government to effectively communicate the need for change. Sharing risk information and identifying potential risk mitigation measures will provide businesses with the tools they need to address changing cybersecurity risks.

- Voluntary industry sector governance mechanisms are sometimes used to stimulate organizations to conform to a set of principles, guidelines, and operations based on best practices, standards, and conformity assessment processes that collectively increase the level of assurance while preserving organizations' brand standing and the integrity of products and services.

    o Do organizations participate in voluntary governance mechanisms?

    AFPM members participate in a variety of voluntary mechanisms, administered by both government and non-governmental organizations. These mechanisms are chosen based upon the facility and risk level.

o Which industries/groups have voluntary governance mechanisms?

AFPM is not a standards-developing organization. Standards-developing organizations such as NIST, ISO, SANS, or other Frameworks (e.g. IEC, UN, EU) which can be implemented by a company, can be considered a "voluntary governance mechanism".

o Do existing voluntary governance mechanisms have cybersecurity-related constraints?

If there are constraints, they would be in unilaterally applying all requirements across all regions globally, especially on encryption controls, backend security and the risk to a country's national security posture.

o What are the benefits and challenges associated with voluntary governance mechanisms?

Benefits: Helping guide those who otherwise do not have the resources to build a custom framework/governance process. Voluntary governance, when supported by compliance and assurance would be the preferred model.

Challenges: An overly prescriptive mechanism could be too restrictive and could lead to a company having security gaps because the company is only following the governance mechanism instead of thinking about security holistically. Similarly, it could lead to the development of costly mitigation measures that, based on facility specifics, are not appropriate for risk mitigation at a specific site.

AFPM looks forward to continuing an open, constructive dialogue with the Department of Commerce on the development of incentives. 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