American
Fuel & Petrochemical
Manufacturers

1667 K Street, NW
Suite 700
Washington, DC
20006

202.457.0480 office
202.457.0486 fax
afpm.org

April 8, 2013

Docket Number 130208119-3119-01
National Institute of Standards and Technology (NIST)
Attn: Diane Honeycutt

RE: AFPM Comments on "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

AFPM, the American Fuel and Petrochemical Manufacturers, appreciates the opportunity to provide comments on the "Developing a Framework to Improve Critical Infrastructure Cybersecurity" Request for Information Notice (RFI).[1] Many AFPM member sites have made considerable investments in cybersecurity infrastructure and follow established standards in the industrial control systems (ICS) and enterprise systems (IT); therefore we have considerable interest in the development of the Framework.

I. General Comments

AFPM appreciates the opportunity to provide comment during the early stages of development of this Framework. Proactively requesting information from stakeholders will provide real value to the NIST.

President Obama's Executive Order 13636 "Improving Critical Infrastructure Cybersecurity" ("Executive Order") emphasized that NIST is to incorporate in the Cybersecurity Framework "industry best practices" as well as voluntary consensus standards, "to the fullest extent possible." In order to achieve these goals, NIST must develop a transparent process that AFPM members can use to obtain federal recognition as Framework-compliant for the best practices that are already in place at member facilities.

In the RFI, NIST posed a number of questions under Current Risk Management Practices, Use of Frameworks, Standards, Guidelines, and Best Practices, and Specific Industry Practices. We address these specific questions below:

[1] 78 *Federal Register* 13024 (February 26, 2013).

II. Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. In addition, NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements. This will assist in NIST's goal of developing a Framework that includes and identifies common practices across sectors.

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Having the right resources in place to conduct cybersecurity is critical. No longer can an operator or control engineer be expected to understand all the complexities of network architecture, system architecture, and other security technologies such as VPN, VLANs, Firewalls, “DMZ’s” between control systems and enterprise systems, Intrusion prevention / Detection and Monitoring Systems.

In addition organizations are in constant need of cybersecurity awareness. This training should educate the user about current threats as well as the general principles to protect themselves and assets. This is especially relevant since training of individuals is often the best deterrent against social media attacks.

Another challenge is in understanding, by conventional IT resources, the differences between a controls environment and commercial IT department. While there are some technologies and concepts that apply equally to both, there are some key differences that help drive cybersecurity efforts.

Finally, a considerable challenge for the industry in the future is multiple regulatory bodies each with similar, but not exactly the same, cybersecurity requirements.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

Some of the greatest challenges AFPM members see include having the appropriate people involved from private and public sectors, willingness by management to do inter-departmental cross training, and differences in key technologies for each sector.

Cross-sector standard approaches often assume that each sector environment is identical to its predecessors or other environments, which may not be the case. The framework development should involve key stake holders that can help to create an architecture that is adaptable to dynamic environments. Rigid standards should not be included in high- level documents due to variations in installations.

Even within a sector, there will be variation. Tools used to run a refinery will differ from those used to run a pipeline, which differ from those used to run a chemical facility. The needs of an integrated oil company will differ from a service company, and what may work for a small single-purpose company may not be sufficient for a large one. The needs could also vary depending on geographic differences. Control objectives will be largely consistent across these segments, but the controls will vary significantly.

3.   Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?

Many AFPM members have developed a security plan to specifically address risk and cybersecurity risk. One example is an enterprise risk management process to identify major risk events that could have a material impact on the company and to ensure the company has systems and processes in place to mitigate those exposures. IT risk is an integral part of the enterprise risk management strategy.

AFPM member companies state that the implementation of a risk management framework will also help create a high level company security plan that includes adaptable standards that are implemented on an operation level to ensure predictable outcomes. This methodology should utilize the strengths of people, processes, and techniques for the primary purpose of safely supporting the strategic goals and objectives of the company.

AFPM member companies also engage senior management in setting the direction and overseeing the risk assessment process as well as ensuring proper mitigation strategies are in place.

4. Where do organizations locate their cybersecurity risk management program/office?

Many AFPM members locate cybersecurity risk in key buildings/offices to obtain timely managerial support and feedback. These include, but are not limited to: the General Counsel's office, the Information Technology organization, and/or an Enterprise Risk Management group.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

Risk is a function of the severity and probability of an injury, liability, loss or any other negative occurrence that is caused by external or internal vulnerabilities and/or assets. Business process risks are assessed based upon a number of factors and weighted based upon the potential cost of various risks. Computing risks are also reviewed as part of an integrated risk management process that considers risks of loss of information integrity, information disclosure, information or processing loss, risks of failing to meet contractual or regulatory requirements, impact on others, and financial consequences. Cybersecurity risks fall under this general computing risks area and are assessed using its framework

Understanding the risks allows industry to focus its security and mitigation efforts appropriately.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

It is a primary element and one of the core components of the overall business risk environments and feeds into an organization's enterprise risk management strategy and program. A company must understand its assets, the risks associated with those assets and importance of the assets. This understanding provides important information so that the company can protect each asset with the necessary layers of protection.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

AFPM members utilize American Petroleum Institute (API), International Society of Automation, (ISA), NIST and other documents for reference material and adapt them to cover various types of environments. AFPM members also consider all governmental recommendations and best practices that are published (e.g. US-CERT, ICS-CERT, TSA and other DHS alerts/publications).

In AFPM member facilities, one would find technologies such as firewalls, physical security measures, Stateful Inspection Firewall Appliances, operating system patching, traditional antivirus, application white listing, event monitoring and mitigation applied on an on-going basis.

Some AFPM members are beginning to invest in more event management concepts to help their companies better respond to potential threats and incidents. Benchmarking and information sharing are used to compare company practices.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

Regulatory requirements that apply to AFPM members include (but are not restricted to): SOX, SEC cyber risk reporting guidance, CFATS (for petrochemical facilities); HIPAA, state data breach notifications, data privacy laws (both domestic and foreign), and various requirements for refining, packaging, and transporting fuels and petrochemicals.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

AFPM member companies must rely on other critical infrastructures in order to manufacture fuel and petrochemical products and to get them to market. These include, but are not limited to: electrical, water, telecommunications and transportation. Many AFPM member facilities require robust network support and cybersecurity efforts that involve interaction with other critical infrastructures.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

The cybersecurity plans in many AFPM member companies incorporate incident response planning guidelines. These guidelines provide both the training and real time assessment of a facility's needs and what further training for staff as well as what new technologies the facility should implement. Many AFPM members run annual incident response drills under various physical and cyber scenarios. In addition, AFPM members have disaster recovery and business continuity plans exist which are also reviewed on a regular basis.

11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?

AFPM member companies are subject to multiple US Federal regulatory bodies (e.g. DHS, OSHA, EPA, etc.) as well as state regulatory bodies.

Depending on the product that the AFPM member company produces, reporting requirements differ. An example is that AFPM members who manufacture petrochemical products must report under CFATS, which incorporates cybersecurity requirements.

12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?

NIST has created several applicable standards which are used in the refining and petrochemical industries. The American Petroleum Institute (API) and the International Society of Automation (ISA) also provide standards and guidelines and both should be utilized to their fullest extent. At a minimum cybersecurity policies and guidelines should include these documents as part of their baseline. In addition, steps should be taken across these industry guidelines to, where possible, maintain some consistency.

Additionally, any standards that are adopted must be dynamic as standards are not static and the requirements called out for in a standard could change over time. NIST must emphasize that the standards in the Framework must be the most current editions.

III. Use of Frameworks, Standards, Guidelines, and Best Practices As set forth in the Executive Order.

NIST states that the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions.

NIST is seeking information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

Per the RFI, AFPM provides information related to the following:

1. What additional approaches already exist?

AFPM members utilize US-CERT, ICS-CERT guidance material, and cybersecurity guidelines developed by trade associations and other organizations.

2. Which of these approaches apply across sectors?

US-CERT alerts, ICS-CERT alerts, best practices and NIST standards could apply across sectors.

3. Which organizations use these approaches?

AFPM members utilize ISA standards in their control systems. Other standards which deal with data relating health care, finance, and other areas are utilized as needed in AFPM member facilities. Additionally, US-CERT and ICS-CERT alerts, NIST standards, and other industry guidelines are followed.

4. What, if any, are the limitations of using such approaches?

Many standards are purposely narrow in scope, only focusing on specific environments and/or goals. These standards are used as a base by AFPM members to build specific facility requirements. Many standards do not address risk outcomes.
Additionally, standards can lag behind technological development as they have to go through a specific process in order to be adopted. It is not usual for the latest revision of a standard to call out technologies that are already dated.

5. What, if any, modifications could make these approaches more useful?

Harmonization of like standards would be helpful to end-users. NIST should emphasize that standards are to be used as a basis from which a facility can build its cybersecurity structure. Further, NIST should work to ensure a timelier and more open approach to developing standards emphasizing information exchange and the use of existing technologies to obtain consensus on standards.

6. How do these approaches take into account sector-specific needs?

An appropriate Risk Management framework considers that risk areas are multi-dimensional and provides an appropriate construct for organizations to make risk mitigation decisions by applying the appropriate process and technology controls. This model provides the flexibility and scalability to be adaptable to any risk situation.

7. When using an existing framework, should there be a related-sector specific standards development process or voluntary program?

All standards have positives and negatives and use should be voluntary, not mandatory. The oil & gas and the chemical sectors have such a diverse collection of companies (large/small, US only/international, integrated/focused on one industry area, service company/oil) that a single standard will not likely suffice. AFPM members are also subject to multiple sectors and under jurisdiction of multiple regulatory regimes both in the US and abroad. It would be better to allow selection of appropriate standards/controls than to force a company to have to implement multiple mandatory requirements.

AFPM emphasizes that each business should be allowed to determine how it will meet the cybersecurity objectives of whichever framework is used. In many cases, sector-specific controls may be appropriate to many companies within the segment. However, each company will be in the best position to know the technologies that they use, and to determine how the controls should be implemented.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

The sector-specific agencies and related sector coordinating councils encourage companies to implement these approaches and best practices by fostering an information exchange and sharing environment. In addition, industry associations can promote collaboration among different sector entities and be the conduit for information to the industry.

9. What other outreach efforts would be helpful?

AFPM members believe that outreach efforts emphasizing education, training, timely bi-directional information sharing, and anonymous communication between companies and government, would be most beneficial. AFPM encourages NIST to use various channels of communication to achieve outreach goals, including industry conferences, webinars, and briefings held in relative proximity to facilities.

IV. Sector Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

1. Are these practices widely used throughout critical infrastructure and industry?

These practices are mature and are utilized by many AFPM members.

2. How do these practices relate to existing international standards and practices?

Many AFPM members have international facilities and must be able to be compliant with both U.S. and International standards. In many cases, standards or practices in one part of the world either directly conflict or are not complimentary with standards elsewhere.

AFPM recommends that any proposed U.S. standards be discussed with International standard bodies (e.g. ISO, IEC) and vice versa.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

AFPM members identify the following as especially critical: Separation of business from operational systems; Identification and authorization of users accessing systems; Monitoring and incident detection tools and capabilities; and Incident handling policies and procedures. All of these practices should be applied using a risk based approach.

Additionally, having well-trained personnel with the latest information is also considered critical by AFPM.

4. Are some of these practices not applicable for business or mission needs within particular sectors?

Applicability of these practices may vary across organizations in a specific sector based on risk factors and situations.

5. Which of these practices pose the most significant implementation challenge?

The challenges to implement these practices will vary across an organization in a given sector based on the specific facility, the current technology deployed and regulatory requirements.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

Standards and guidelines are used to as the base of a framework to define how a given practice is applied to varying technology throughout a facility. Standards and guidelines also define the appropriate implementation and testing procedures to ensure controls are operating effectively from facility to facility.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

AFPM members have excelled in improving their information security capabilities. Many AFPM members' budgets include securing new technologies, business continuity and disaster recovery.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

While there are escalation processes used by AFPM members, there is no one escalation process that covers both the refining and petrochemical industries Alerts received from ICS-CERT or from classified briefings can put the escalation process in motion.

AFPM members also recognize the role that industry vendors play in alerting the industry to a potential cybersecurity issue.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

As long as the framework incorporates an information classification and protection program, there should be no risks to privacy and civil liberties. States already have existing privacy and breach laws that provide coverage for personally identifiable information. However, AFPM strongly urges that there be a balance between privacy and monitoring.

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

The Framework must be globally implemented and recognize the various regional standards and laws.

11. How should any risks to privacy and civil liberties be managed?

Risks to privacy and civil liberties should be managed the way any other risk should be managed, by ensuring and routinely testing, that appropriate controls are designed, implemented and monitored for effectiveness.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Employee education and awareness training should be a part of the framework. Given that the human element of any cybersecurity program progressively poses risk to the sector assets, periodic reminders are essential to the success of any program. In parallel with education and awareness, is the inclusion of tabletop exercises and simulations.

Further, any practice that is adopted must be routinely reviewed and tested to ensure that it is compatible with the current threats and technologies.

AFPM looks forward to continuing an open, constructive dialogue with the National Institute of Standards and Technology of the development of this 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