AMERICAN PETROLEUM INSTITUTE

Aaron P. Padilla
Senior Advisor, Tax and Accounting Policy

1220 L Street, NW
Washington, DC 20005-4070
Telephone (202) 682-8468
Fax (202) 682-8408
Email padillaa@api.org
www.api.org

October 10, 2014

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: RFI regarding "Experience With the Framework for Improving Critical Infrastructure Cybersecurity"

Dear Ms. Honeycutt:

The American Petroleum Institute (API) welcomes the opportunity to respond to the National Institute of Standards and Technology's (NIST) Request for Information, issued by the Department of Commerce in the Federal Register on August 26, 2014, to ascertain awareness and initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework") published February 12, 2014.

API is a national trade association that represents all segments of America's oil and natural gas industry. Its more than 600 members include large integrated companies, exploration and production, refining, marketing, pipeline, and marine businesses, and service and supply firms.

There is significant awareness of the "Framework" within the oil and gas industry as several member companies have used or are considering use of the Framework as a tool to review and identify gaps within existing security practices, to facilitate project prioritization and/or to frame risk assessments. A key benefit of early adoption is the raising of the visibility of cybersecurity issues both within corporations and within the country. The increased visibility within corporations encourages cybersecurity conversations and interactions that may be more beneficial than gap assessments. At the country level, the Framework provides a national focus on these cybersecurity issues in lieu of any national cybersecurity legislation and engenders confidence that United States is effectively addressing cybersecurity. Key issues to address as priorities include data analytics, international cooperation and harmonization, and supply chain risk management. Congressional passage of comprehensive cybersecurity legislation that encourages information sharing and liability protection to organizations that participate in sharing processes would be helpful, as would considerable dialogue on how to ensure alignment of global cybersecurity protocols and directives to prevent disruptions to global commerce and facilitate supply

chain management. Lastly, while not actually part of the Framework itself, completing a well-defined incentive system would induce “fence-sitting” companies to facilitate Framework implementation.

The following attachment provides specific answers to each of the questions posed in the RFI. API looks forward to working with NIST to clarify and build upon these responses to help create the cybersecurity Framework.

Should you have any questions or would like to discuss further, please feel free to contact me at (202) 682-8468 or PadillaA@api.org.

Sincerely,

Aaron Padilla
Senior Advisor, Tax and Accounting Policy
API

Encl: API Response to August 26, 2014 National Institute of Standards and Technology (NIST) Request for Information (RFI) on Experience With the Framework for Improving Critical Infrastructure Cybersecurity

American Petroleum Institute (API) Information Technology Security Subcommittee (ITSS) Response to August 26, 2014 National Institute of Standards and Technology (NIST) Request for Information (RFI) on Experience With the Framework for Improving Critical Infrastructure Cybersecurity

Current Awareness of the Cybersecurity Framework

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

There is significant awareness of the Framework based upon interaction with personnel working within the oil and natural gas industry. Several companies have begun to use the Framework as a tool to review and identify gaps within existing security practices while others have used the Framework to facilitate project prioritization or to frame risk assessments. Despite broad awareness and even with additional companies considering use, there has not been widespread usage of the Framework at this time.

2. How have organizations learned about the Framework? Outreach from NIST or another government agency, an association, participation in a NIST workshop, news media? Other source?

The Framework has been mentioned in many newspaper articles and on television although these references lack sufficient detail to provide much impetus for adoption. The American Petroleum Institute's IT Security Subcommittee (API ITSS) has discussed the Framework within its meetings and plans to have sessions at the upcoming API Cybersecurity Conference in November. Outreach by NIST and DHS in a series of awareness sessions have also been well attended by members of the oil and gas community. Significant time and resources have been expended by the Oil and Natural Gas Sector Coordinating Council (ONG SCC), working with Department of Energy (DoE) on implementation guidance for the sector. Many companies within the Oil and Natural Gas Sector sent delegates to the NIST Framework development workshops and provided input to the Framework.

3. Are critical infrastructure owners and operators working with sector-specific groups, non-profits, and other organizations that support critical infrastructure to receive information and share lessons learned about the Framework?

Significant time and resources have been expended by the Oil and Natural Gas Sector Coordinating Council (ONG SCC), working with Department of Energy (DoE) on implementation guidance for the sector. The American Petroleum Institute's IT Security

Subcommittee (API ITSS) has had several discussions of this topic in its meetings and plans to have sessions on the Framework during their upcoming API Cybersecurity Conference. Outreach by NIST and DHS in a series of awareness sessions have also been well attended by members of the oil and gas community.

Most efforts, though, have been internal to individual companies as there have been few attempts to extend Framework use/awareness to business partners or others within the supply chain.

4. Is there general awareness that the Framework:

a. Is intended for voluntary use?

Yes

b. Is intended as a cyber risk management tool for all levels of an organization in assessing risk and how cybersecurity factors into risk assessments?

Not really. Most organizations will use the Framework within the portions of their organizations responsible for risk management, not at every level in an organization. It is not really suitable for use on the front lines where the detailed controls selected by an organization will be implemented. Use of the Framework is NOT a good use of implementers' time; they should be implementing the adopted controls. Those within an organization who have access to the detailed referenced controls frameworks are the only ones who can effectively use the entire framework. Those personnel should then work within their organization to incorporate the terminology and selected controls that their organization will actually use to all appropriate personnel.

c. Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?

Yes

5. What are the greatest challenges and opportunities—for NIST, the Federal government more broadly, and the private sector—to improve awareness of the Framework?

The fact that the much discussed incentives have not materialized is a major factor. While some companies have adopted proactively, others are waiting to see what incentives may be made available. Getting all sector specific agencies to fully incorporate the Framework in their communications and (where applicable) regulations with their sector would be highly effective.

Having all government entities fully embrace the Framework would send a powerful message to industry that using the Framework is not only possible, but effective.

6. Given that many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, what is the level of awareness internationally of the Framework?

As noted in the question, multi-national companies, as they adopt the Framework internally, will drive use and awareness outside of the United States. Some efforts, like the proposed European Union Network and Information Security (NIS) directive effort have begun to reference the Framework. While international awareness is growing, most outside of the United States have not reviewed the Framework in detail nor considered updating their own frameworks based upon it. DHS and/or NIST should expend resources to identify the entities around the world that are actively setting cybersecurity / IT standards and proactively contact them to see if there are ways to harmonize their frameworks with the U.S. Framework. Such harmonization should be technically possible as the Framework is on multiple (international) standards (the informative references). Encouraging a voluntary approach that emphasizes sharing of cybersecurity information between governments/law enforcement and industry would be helpful.

7. If your sector is regulated, do you think your regulator is aware of the Framework, and do you think it has taken any visible actions reflecting such awareness?

Oil and natural gas companies operate in several regulated areas. Regulators do seem to be aware of the Framework. It is less clear that they are prepared to adopt the Framework as the basis for their future regulations. For example, DoE's approach is largely around allowing existing processes and the Framework processes to be used interchangeably rather than changing existing processes to fit within the Framework.

8. Is your organization doing any form of outreach or education on cybersecurity risk management (including the Framework)? If so, what kind of outreach and how many entities are you reaching? If not, does your organization plan to do any form of outreach or awareness on the Framework?

Virtually all oil and natural gas companies have had cybersecurity awareness programs that incorporate periodic communications as well as mandatory cybersecurity training. Most of these programs, many have which have been in place for years, are in addition to existing risk management processes that have been in place for decades. Externally, companies have been working with a variety of organizations that are actively promoting cybersecurity awareness, include API, DoE, US Chamber of Commerce, and the Business Roundtable. During the development of the Framework, awareness was raised about how organizations could participate in the development process. Since release of the framework, awareness of the Framework and how organizations may want to utilize it has been included in these communications.

9. What more can and should be done to raise awareness?

In many cases, the awareness programs that are currently in place are "preaching to the choir" in the sense that the organizations that are actively participating are already cybersecurity

aware and already have appropriate processes and controls in place. The Department of Energy Framework implementation guidance document is one means to raise awareness with companies which lack robust security programs. Release of an incentive program may provide an opportunity for getting these organizations' attention.

Having Congress pass comprehensive cybersecurity legislation that encourages information sharing and liability protection to organizations that participate in sharing processes would be helpful, as would considerable dialogue on how to ensure alignment of global cybersecurity protocols and directives to prevent disruptions to global commerce and facilitate supply chain management.

Experiences With the Cybersecurity Framework

1. Has the Framework helped organizations understand the importance of managing cyber risk?

Most companies are already aware of the importance of managing cyber risk but the framework does provide a common language for discussing cybersecurity.

2. Which sectors and organizations are actively planning to, or already are, using the Framework, and how?

Several oil and natural gas companies have begun to use the Framework as a tool to review and identify gaps within existing security practices while others have used the Framework to facilitate project prioritization or to frame risk assessments. The Framework, by providing a common language, has also been used as a means to communicate cybersecurity issues within companies and to management.

3. What benefits have been realized by early experiences with the Framework?

A primary benefit of the Framework is the common language for discussing cybersecurity and allows entities to provide comfort/confidence regarding compliance with security controls.

The Framework enables gap assessments and allows companies to recheck existing cybersecurity controls. The ability to identify gaps and ultimately close them improves the security of the company which itself is a benefit.

The Framework raises the visibility of cybersecurity issues both within corporations and within the country. The increased visibility within corporations encourages cybersecurity conversations and interactions which may be more beneficial than gap assessments. At the country level, the Framework provides a national focus on these cybersecurity issues in lieu of any national cybersecurity legislation and engenders confidence that US is doing the right thing for security

4. What expectations have not been met by the Framework and why? Specifically, what about the Framework is most helpful and why? What is least helpful and why?

Most helpful elements of the Framework are the mapping to informative references and the common view of cybersecurity. The Framework itself, while designed for critical infrastructure, is general enough that it is being applied to other environments.

As stated in the answer to question three, the Framework provides a focus on cybersecurity that engenders additional discussion and work within companies and the country on relevant issues.

The "tiers" are perhaps the least useful element of the framework. The final version reset the tiers to the enterprise level, away from the categories/sub-categories as intimated in preliminary versions. Setting an enterprise level is fine but there is no information or guidance as to how these levels reflect into categories/subcategories and consequently, one tends not to even consider the tiers when identifying gaps and potential solutions. Setting the organizational tier level is basically unused work.

The lack of differentiation between the Respond and Recover functions creates additional problems.

Lastly, while not actually part of the Framework itself, the absence of a well-defined incentive system is also not helpful, particularly for companies who might have been awaiting such incentives to facilitate Framework implementation.

5. Do organizations in some sectors require some type of sector specific guidance prior to use?

Corporations with established cybersecurity programs and resources likely will not require sector specific guidance. The aforementioned Department of Energy guidance document will assist organizations lacking such programs and resources.

6. Have organizations that are using the Framework integrated it with their broader enterprise risk management program?

Yes, particularly those with established programs.

7. Is the Framework's approach of major components—Core, Profile, and Implementation Tiers—reasonable and helpful?

The Core and Profile components are reasonable and helpful. As noted above, Tier, because of the absence of ties to the other components, seems useless.

8. Section 3.0 of the Framework ("How to Use the Framework") presents a variety of ways in which organizations can use the Framework.

a. Of these recommended practices, how are organizations initially using the Framework?

Gap assessment, comparing existing controls against the Framework, is the most common use case with communications (common language) a close second. There are isolated instances of more innovative use including project prioritization and framing risk assessment questions for specific environments (like process control.)

b. Are organizations using the Framework in other ways that should be highlighted in supporting material or in future versions of the Framework?

One item to be considered is replacing myriad external service provider review questionnaires with one based on the Framework. This would drive consistency with other (industry) organizations and might facilitate corporation/industry interaction (as there would be a common language if not common set of questions for vendors to answer.)

c. Are organizations leveraging Section 3.5 of the Framework ("Methodology to Protect Privacy and Civil Liberties") and, if so, what are their initial experiences? If organizations are not leveraging this methodology, why not?

Oil and natural gas organizations are not leveraging this section much because multi-national firms already have privacy programs in place to deal with privacy legislation from the US, Europe, and other jurisdictions.

d. Are organizations changing their cybersecurity governance as a result of the Framework?

For companies with established security programs, there is probably more integration or augmentation than replacement.

e. Are organizations using the Framework to communicate information about their cybersecurity risk management programs—including the effectiveness of those programs—to stakeholders, including boards, investors, auditors, and insurers?

The Framework is being used as a communications vehicle and in some cases, is being recommended over other methodologies as the common communications platform.

f. Are organizations using the Framework to specifically express cybersecurity requirements to their partners, suppliers, and other third parties?

As noted above, this is under consideration but to date, industry companies have focused the Framework use internally and not on their supply chains and partners.

9. Which activities by NIST, the Department of Commerce overall (including the Patent and Trademark Office (PTO); National Telecommunications and Information Administration (NTIA); and the Internet Policy Taskforce (IPTF)) or other departments and agencies could be expanded or initiated to promote implementation of the Framework?

The Department of Commerce should continue to "advertise" the Framework and provide NIST adequate resources to maintain it.

10. Have organizations developed practices to assist in use of the Framework?

The primary document within oil and natural gas (and actually within the energy sector itself) is the Department of Energy Framework Implementation Guidance document.

Roadmap for the Future of the Cybersecurity Framework

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?

The Roadmap identifies the most important cybersecurity areas although we do not believe all to be equal in value/impact. We would rank data analytics, international aspects, and supply chain risk management as the upper tier of items to address. Automated indicator sharing, conformity assessment, and cybersecurity workforce would occupy the middle tier with authentication and technical privacy management taking the lowest eschelon.

2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?

The Framework should directly address the need for reassessment of risks (1) when changes occur and (2) at specified intervals.

The Framework should document a requirement for assessing the impact of new standards

The Framework should specifically address the need for multidisciplinary teams including expertise from outside the immediate unit

The Framework should document the need for a formal feedback mechanism to learn about significant changes at external service providers. Vendor agreements should be covered as more companies use third parties/public cloud for services. These are probably part of supply chain but need to be called out. Cloud computing itself should be addressed within the Framework. In preparing the response to this RFI, API members noted that no Cloud Security Alliance documents, neither Security Guidance nor Cloud Controls Matrix, are included as informative references.

Internet of things should be covered as well. As more traditionally non-IT items, like light bulbs, become connected (and network nodes), cybersecurity will shift more toward operational (control system) security and the Framework will need to assure adequate coverage.

Lastly, it would be very helpful if all of the information references could be made available to all Framework users at no cost so that they may be used for the purposes of performing assessments. Many small or medium size business may not be able to afford to purchase licenses of some of the informative references and consequently are restricted from using these potentially useful documents unless there were some means to make these available for free.

3. Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?Show citation box

Just as the European Union (EU) has acknowledged the Framework as it develops its Network and Information Security directive, NIST should acknowledge the EU work and incorporate relevant changes into the Framework. Multi-national corporations run critical infrastructure in the US, Europe, and elsewhere around the world and harmonized frameworks would go a long way in helping companies appropriately secure these resources.

The Framework also should acknowledge the trend outside of the US to localize specific information in-country as such laws can affect security control implementation.