AMERICAN PETROLEUM INSTITUTE

Aaron P. Padilla
Senior Advisor, International Policy

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

February 9, 2016

Diane Honeycutt
National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: **API Response to NIST RFI on Views on the Framework for Improving Critical Infrastructure Cybersecurity**

Dear Ms. Honeycutt:

The American Petroleum Institute (API) welcomes the opportunity to comment upon the NIST Request for Information (RFI) on Views on the Framework for Improving Critical Infrastructure Cybersecurity.

API is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 650 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

Cybersecurity is a priority for the oil and natural gas industry and API members. As operators and service providers of energy critical infrastructure in the United States and globally, protecting networks from cyber-attacks is a priority of API's members.

API remains strongly supportive of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. The Framework has been widely-used by the oil and natural gas industry represented by API's member companies. We welcome the opportunity to share our perspectives on the Framework in the following pages, answering each of the RFI questions.

Sincerely,

Aaron Padilla
Senior Advisor, International Policy
API

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	The American Petroleum Institute (API) is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 650 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry. They are producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry. Cybersecurity is a priority for the oil and natural gas industry and API members. As operators and service providers of energy critical infrastructure in the United States and globally, protecting networks from cyber-attacks is a priority of API's members. API member companies manage cybersecurity with oversight from Boards of Directors and Senior Executives. Consistent with this, member companies have prioritized cybersecurity as a policy issue at API's CEO-led Board of Directors. API member companies also convene on cybersecurity in two API committees: one comprised of Chief Information Officers (CIOs) and another comprised of Chief Information Security Officers (CISOs) and other cybersecurity experts and cybersecurity threat analysts.	
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	Multiple organizations (as indicated above), ranging from many API member companies using the Framework in a variety of different ways and some not using the Framework. An industry survey concluded in the third quarter of 2015 found about two-thirds of 53 oil and natural gas companies are using the Framework in some manner.	

#	Question Text	Response Text	References
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	The aforementioned industry survey of 53 oil and natural gas companies found half of those using the Framework have integrated it into the corporate cybersecurity program while the other half uses the Framework for specific purposes. --77% of respondents use the Framework to evaluate cybersecurity capabilities and programs --69% use the Framework to prioritize cybersecurity programs --48% use the Framework to facilitate cybersecurity communications (via common language/taxonomy) --32% use the Framework to benchmark cybersecurity performance versus external peers --25% use the Framework to evaluate external suppliers/contractors Industry members have used the Framework to map internal controls, help with incident investigation, testing incident response, and to evaluate critical control systems. One company enlisted a third party to assess the company against the Framework with then used this information to benchmark performance/capability against peers and with other industries. Another company has used the Framework to track completeness of its controls against the broader strategic context; this company is about to initiate an enterprise wide effort that will use Framework and associated tools to determine maturity targets and track future progress. One company has used the Functions and Categories to structure cybersecurity activity and the Sub-categories as a check for policy and assurance activities.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	API member companies offer these examples of utilizing specific portions of the Framework: --The Framework is an excellent tool for measuring current Profile and developing actions forward to change the Profile and fill in gaps as needed. --The Framework Core has served as a basis for external cybersecurity communications both within the Oil and Natural Gas industry and outside. --The Framework has also been used for internal communications with the functions particularly useful to frame messages to senior management. --One company is using the Functions and Categories to structure and defined IT services and IT service offerings to internal customers.	
5	What portions of the Framework are most useful?	The Framework Core, particularly the Functions and Categories, are the most useful providing the common taxonomy for communications and security evaluation. The Informative References are useful providing a correlation with other frameworks.	

#	Question Text	Response Text	References
6	What portions of the Framework are least useful?	The Framework Tiers are difficult to understand and of little signfiicance (particularly when set at a corporate/enterprise level). There is little difference among the Subcategories within the Respond and Recovery Functions. One company reports that Implementation tiers and privacy methodology have not been used to date. Implementation tiers were unhelpful as they caused confusion when it came to measuring maturity of capabilities, leading to results that did not easily cross-reference with other assessments.	
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	The Framework lacks depth for SCADA/ICS environments. Specific guidance for ICS (as outlined in NIST SP 800-82) would be beneficial to the Oil and Natural Gas Industry. One company's use of the Framework has been limited to where other existing frameworks are also in use. Where an existing framework is in use, mappings between the two framewoks have been used to support reporting. This mapping and reporting has been done internally and when working with third parties. One company is altering Subcategory names to make these more representative of existing company terminology and thereby easier for its disparate business units to consume.	

#	Question Text	Response Text	References
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	The Framework has reduced cybersecurity risk through better cybersecurity communications and an ability to identify areas of improvement. The Framework, particularly via the five Functions, provides a template for discussing cybersecurity with senior management. These communications and the entire process for creating the Framework, starting with the President's Executive Order, has raised awareness among senior management in the oil and natural gas industry and highlighted the importance of cybersecurity in protecting critical infrastructure. Senior management in turn has increased spending and effort on cybersecurity which is intended to lower risk. The increased visibility of the Framework among senior management limited cybersecurity staff reductions and other cost cutting which normally would have occurred with the reduction in oil prices. One company reports that the Framework has helped categorize cybersecurtiy activities in a way that is easily recognizable between industries, which has helped communication of the capabilities and improvements of cybersecurity initiatives that were already in place. Regarding metrics, one oil and natural gas company reports that the Framework has been used to create a matrix of cybersecurity strengths and areas of improvements. This information has been factored into the budgeting and planning processes to improve cybersecurity posture. Another company reports that metrics like "Vulnerabilities per Asset" are reported monthly and show improvement.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	In order to prevent duplication of regulatory requirements, Framework Profiles could be developed for any potential different regulatory processes as the first step toward understanding the role of cybersecurity in a given industry sector or sub-sector or aspect of critical infrastructure. NIST is already doing this with the Coast Guard. Such use of the Framework Profiles helps to align regulatory regimes to a common base which would help to identify duplication while also facilitating implementation by those regulated. Those companies using the Framework internally would be able to map easily a regulation to be implemented by incorporating the Framework Profile(s) into corporate process(es). Those regulated by multiple regimes would be able to use the Framework to identify all requirements (assuming the regulation were informed by Framework Profiles) and identify like elements required by different regulations. Absent Framework Profiles, regulatory regimes still could be mapped to the Framework. A gap report could be developed showing where the Framework may already prompt a company to manage cybersecurity areas of concern to a regulatory agency.	

#	Question Text	Response Text	References
10	Should the Framework be updated? Why or why not?	The Framework must be a living document as neither information technology nor cybersecurity threats are static. Companies will continue to deploy new technologies and move into new environments; threat actors will continue to upgrade their attacks to gain advantage. However, API member companies advocate that NIST limit the changes to the Framework at this time, which will allow for more entities to use it as is and for those already using it to mature in their use of it.	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	API member companies offer the following opportunities for changes, not necessarily immediately (see above), but at an appropriate time: --As noted above, the current Framework lacks specificity for ICS controls and a mapping for the regulatory requirements of different government agencies. --The "Tiers" concept should be eliminated or restructured into something more meaningful/useful. --Other authoritative sources should be reviewed to ensure complete coverage of references. One example is to add COBIT 5 APO13.12 as an informative reference to ID.GV-2. --Suggested new sub-categories: (1) ・ID-AM-7: Documentation (for software, hardware, devices, procedures, networks, diagrams and dataflows) is identified and inventoried; (2) ・PR.PT-5: Unnecessary applications and services are removed/disabled to reduce attack surface. --Cyber threat intelligence has very limited coverage given the potential value from doing this activity. --Awareness & Training could benefit from being made more prominent. --Aligning the implementation tiers to a commonly recognised maturity model (like CMMI) would help industry understand current capability levels and make smarter decisions. It would also fit with most other similar assessments and avoid the potential for confusion over implementation tiers and maturity. --We have identified multiple gaps as indicated in Annex A, immediately following the response to the RFI's 25 questions.	
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?	A self-assessment tool would be a helpful addition. A primary Subcategory should be identified for those informative references which map to multiple Subcategories.	
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	Most of the companies in the Oil and Natural Gas sector have adopted the Framework Core as is from the existing document. Consequently, we do not have any unique approaches that need to be added to the document.	

#	Question Text	Response Text	References
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	The consensus among API member companies is that there is no pressing need to use nine areas identified by NIST in its Framework-related "Roadmap" at this time to inform Framework updates.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Any updates should be published in a completely new, separate version similar to the way ISO handles updates to 27000. This approach allows entities to decide when to switch to the newer version on their own time as those using the older version could continue to use it. Release notes documenting changes between the versions should be included with the new version as this can help entities identify specific changes.	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	Most entities within Oil and Natural Gas using the Framework have simply read the Framework document and have not used or relied on other comunications or information.	
17	What, if anything, is inhibiting the sharing of best practices?	With the passage of the Cybersecurity Act of 2015, few barriers remain that inhibit the sharing of best practices. The Oil and Natural Gas sector has been discussing best practices through the American Petroleum Institute (API) for at least 15 years. The Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC) launched in 2014 and provides more formal means for sharing information. Some limitations exist for sharing best practices: sensitivity over the nature of securtiy controls, the terms of non-disclosure agreements and concerns about the potential repercussions in the event of an incident.	
18	What steps could the U.S. government take to increase sharing of best practices?	The government can encourage best practice sharing through the ISACs and trade assocations. Of additional benefit is the marketing of the Framework to non-US locations; many Oil and Natural Gas sector companies are multi-nationals and having Framework used both in the US and outside the US facilitates the implementation of multinational companies' cybersecurity programs. The US Government could also do work to publish an anonymized aggregation of best practices.	

#	Question Text	Response Text	References
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	Additional programs may not be necessary. As noted above, oil and natural gas companies have been sharing through the API and informally for years. The passage of the Cybersecurity Act of 2015 and the founding of the ONG-ISAC in 2014 provide additional impetus in this area. API members encourage NIST to continue to reach out to the private sector to gain input on potential enhancements to the Framework from real-world experiences of implementation and also for innovation in the structure of the Framework and any maturity levels that get defined to ensure that maturity expectations continue to evolve. Regarding peer recognition, API member companies do not support a cybersecurity "Baldridge" award, as it would be akin to painting a target on the back of the recognized organization.	
20	What should be the private sector's involvement in the future governance of the Framework?	The private sector should always have the ability to provide input on the Framework. The current means, through NIST's workshops and RFIs, are sufficient.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	Most industry members believe NIST has done an effective job managing the Framework and advocate that NIST retain this responsibility. NIST historically has been effective obtaining input from the private (and public) sector. NIST is well-placed in this role also because many organizations use other NIST standards and/or publications internally. There is some fear that if NIST transitioned some or all of the Framework elsewhere, the new organization may not as actively gather private input or the Framework may become a purchase-only document which would defeat the purpose.	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	API member companies' preference, absent any concrete proposal, is for all Framework governance to remain with NIST.	

#	Question Text	Response Text	References
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	All of these have problems. A non-profit will have to determine some means of funding continuing updates to the Framework. A for-profit will need to make money on the venture. Each of these implies that the Framework may need to be purchased in the future, which will limit use (smaller firms may not want or could not afford to buy initial versions and periodic updates) and could then put critical infrastructure at increased risk. Multinational organizations would be better for global companies as these might haver a better chance of getting more adoption of the Framework across the world. Standards organizations tend to have relatively long development and approval time frames (ISO is about five years) because of the complexity of creating and reaching consensus on updates, and this may lessen the value of the Framework due to the fast-evolving nature of cybersecurity.	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	Standards organizations tend to have relatively long development and approval time frames (ISO is about five years) because of the complexity of creating and reaching consensus on updates, and this may lessen the value of the Framework due to the fast-evolving nature of cybersecurity.	
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	The transition partner would need to do all that NIST currently does, i.e., have the capacity to elicit and process private and public input and create/maintain a document that is available to end users at no cost.	

Gap #	Function.Category	Gap	Recommended Reference (if any)
1	Identify.Asset Management	Corporate vs. Non-corporate devices is not addressed for asset management.	NIST SP 800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise
2	Identify.Asset Management	Need clarity on whitelisting. Higher level of maturity would include whitelisting.	NIST SP 800-167: Guide to Application Whitelisting (as of January, 2016, still in draft)
3	Identify.Asset Management	No specification for how often asset management activities are to occur. "On a regular basis" is not descriptive enough.	
4	Identify.Governance	Relevant external parties/third parties is not defined.	
5	Identify.RiskAssessment	Risk Assessments for the Cloud environment are not discussed	Cloud Security Alliance
6	Protect.AccessControl	No discussion of Federation or Federation architecture.	API Trust Framework (forthcoming)
7	Protect.AccessControl	A Network Protection/VPN-Firewall Reference Architecture is needed.	1) Trusted Internet Connections Reference Architecture Document v2.0 October 1, 2013 2) NIST SP 800-47: Security Guide for Interconnecting Information Technology Systems August, 2002
8	Protect.DataSecurity	No discussion of encryption standards.	1) NSA Types provided 2) NIST SP 800-111: Guideline to Storage Encryption Technologies for End User Devices

Gap #	Function.Category	Gap	Recommended Reference (if any)
9	Protect.DataSecurity	No discussion of key ownership.	NIST SP 800-57: Recommendation for Key Management – Part 1: General (Revision 3) July, 2012
10	Protect.Information Protection	Cabling security discussion is incomplete.	ISO/IEC 27002, Section 11.2.3.
11	Protect.Information Protection	Incomplete discussion of secure backups.	1) NIST SP 800-111: Guideline to Storage Encryption Technologies for End User Devices November, 2007 2) NIST SP 800-123: Guide to General Server Security July, 2008
12	Protect.Maintenance	No maintenance reference architecture provided. For example, the need for protecting information in transit is not discussed.	Configuring and Managing Remote Access for Industrial Secure Systems November, 2010
13	Detect.AnomaliesEvents	No thresholds for triggering alerts were documented.	
14	Detect.SecurityContinuous Monitoring	No discussion of breach notifications from third parties.	
N/A	Protect.Protective Technology	No Gaps	
15	Detect.DetectionProcesses	How privacy regulations apply to third parties is not discussed.	
16	Recover.Communications	No mention of incident coordination with a third party.	
N/A	Respond.Analysis	No Gaps	
17	Respond.Communications	Inadequate discussion of guidelines for response communications with third parties. They are adequate for an internal response function.	