energy API

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

Submitted via cybercommission@nist.gov

September 9, 2016

Nakia Grayson
National Institute of Standards and Technology
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Subject: **API Response to RFI from the President's Commission on Enhancing National Cybersecurity**

Dear Ms. Grayson:

The American Petroleum Institute (API) welcomes the opportunity to comment upon the Request for Information (RFI) from the President's Commission on Enhancing National Cybersecurity. API is the only national trade association that represents all aspects of America's oil and natural gas industry. Our more than 640 corporate members, from the largest major oil company to the smallest of independents, come from all segments of the industry.

Cybersecurity is a priority for the oil and natural gas industry. API member companies manage cybersecurity as an enterprise risk, the highest level of prioritization, with oversight from Boards of Directors and Senior Executives. 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, which are producers, refiners, suppliers, pipeline operators and marine transporters, as well as service and supply companies that support all segments of the industry.

API member companies support the President's focus on cybersecurity and the work of the Commission. API supported the Commission's July 2016 meeting in Houston. At this meeting, API was represented by one of its member companies, ExxonMobil, through the presentation by Scott Robichaux, Cyber Security Center of Excellence (CoE) Manager.

We do not address every topic in the RFI. Instead, API's comments are oriented around five key cybersecurity policy principles that API members advocate for the Commission and the next President and his or her administration to prioritize, as summarized below in an Executive Summary and then explained in more detail in the following pages.

EXECUTIVE SUMMARY

API member companies support President's focus on cybersecurity and the work of the President's Commission on Enhancing National Cybersecurity. As operators and service providers of energy critical infrastructure in the United States and globally, protecting assets from cyber-attacks is a priority of API's members.

1. **API member companies urge policy makers to take a measured and coordinated approach to any potential new cybersecurity laws or regulations for industry.**
   Challenge: Often, current policy making is not helpful for industry because it would introduce prescriptive compliance requirements or mandate incident reporting, neither of which serve industry well in managing cybersecurity risk.
   Solution: API urges the Commission to recommend that the next President undertake a cautious, measured and coordinated inter-agency approach to cybersecurity policy making (1) that takes into account the ongoing work and existing compliance obligations of companies to manage risks (including cybersecurity) and (2) that is based on the Cybersecurity Framework, as developed by NIST.
2. **API member companies support the Cybersecurity Framework as the pre-eminent standard for companies' cybersecurity programs and for policy making globally.**
   Challenge: Companies and government policy makers seek a common reference to align their own and others' efforts on cybersecurity.
   Solution: API urges the Commission and the next President to promote the Cybersecurity Framework, in the US and globally, as *the key* policy reference and tool because it is (a) comprehensive, (b) a risk management approach, (c) scalable to different types and sizes of companies, and (d) widely used across industry.
3. **API member companies believe that the private sector should retain autonomy and the primary responsibility for protecting companies' assets against cyber-attacks.**
   Challenge: Respective roles and responsibilities in cybersecurity between the government and private sector are still being solidified.
   Solution: API urges the Commission to recommend to the next President that the private sector retain the autonomy and responsibility for protecting companies' assets, which has served industry well by incentivizing significant investments, innovations and flexibility from companies, service providers, suppliers and cybersecurity vendors to address dynamic cyber threats.
4. **API member companies believe that governments should have the primary responsibility for deterring and preventing cyberattacks by nation states and criminals against the private sector.**
   Challenge: The private sector faces the threat of cyber-attacks from a variety of actors, especially nation states and organized criminal elements, seeking to steal intellectual property and/or compromise assets such as networks, industrial control systems (ICS), etc.
   Solution: API urges to Commission to recommend that the US government continue work and investment to deter and counter international malicious cyber actors that attack the private sector.
5. **API member companies support voluntary collaboration and information sharing between the private sector and government.**
   Challenge: The private sector needs actionable cyber threat indicators from US government sources.
   Solution: API urges the Commission to continue to emphasize the importance of information sharing and to recommend that the next President continue ongoing efforts to make information sharing operational.

1. **API member companies urge policy makers to take a measured and coordinated approach to any potential new cybersecurity laws or regulations for the oil and natural gas industry, ideally based on a common understanding with industry on risks and based on the Cybersecurity Framework.**

API member companies urge the Commission to recommend caution and coordination with regards to further policy making, including regulation, regarding cybersecurity in the private sector. First, API advocates a cautious, measured approach that takes into account the ongoing work and existing compliance obligations of companies to manage risks (which include cybersecurity risks). Policy making needs to understand the complexities of cybersecurity risk management within and across companies. One-size-does-not-fit-all for companies and cybersecurity, so prescriptive policies and regulations with static compliance requirements do not serve industry well in managing cybersecurity risk. API urges the next Presidential Administration to strengthen dialog with industry so that policy makers understand well the best practices and the current state of cybersecurity risk management in the private sector – before policy makers continue with or develop any new laws and regulations on cybersecurity. API also urges policy makers to consider opportunities when the most effective government role regarding cybersecurity of the private sector may be gathering and sharing best practices in cybersecurity, to strengthen dialog and coordination among companies and government agencies.

Second, API advocates a coordinated approach among government entities. The current trend of policy making on cybersecurity is for various federal agencies and Congress all to pursue separate policies. API strongly urges the next President to oversee coordination and consistency across agencies and jurisdictions, rather than disconnected and piecemeal policy making efforts.

API believes that some current policy making and public policy ideas are not the right approaches because they would introduce prescriptive compliance requirements or mandate incident reporting. Laws and regulations with prescriptive controls have the potential to become obsolete rapidly because the pace of changing cybersecurity threats is far quicker than the pace of crafting and updating prescriptive controls. In addition, prescriptive controls may cause companies to divert resources from other, more effective cybersecurity risk management activities. Instead, API recommends that any policy making be oriented around the NIST Cybersecurity Framework and its risk-based approach.

2. **API member companies support the Cybersecurity Framework, developed by NIST, as the pre-eminent standard for companies’ cybersecurity programs and for policy making globally.**

API member companies urge the Commission and the next President to promote the Cybersecurity Framework as *the key* policy reference and tool because it is (a) comprehensive, (b) a risk management approach, (c) scalable to different types and sizes of companies, and (d) widely used across the oil and natural gas and other industry sectors.

Oil and natural gas companies are using the Cybersecurity Framework extensively – to evaluate cybersecurity capabilities and programs, to prioritize cybersecurity programs, to facilitate cybersecurity communications (via common language/taxonomy), to benchmark cybersecurity performance versus external peers and to evaluate external suppliers/contractors. One API member company has mapped its entire global cybersecurity program to the Cybersecurity Framework. Another API member company is integrating the Cybersecurity Framework into its internal policies and rewriting its company controls and standards with the Cybersecurity Framework as the uppermost part of the controls/standards hierarchy. Another API company has conducted a third party gap analysis of its current cybersecurity program against the Cybersecurity Framework.

API member companies also urge the Commission and next President to promote the Framework globally. Many API member companies operate globally and face the challenge of simultaneous compliance in multiple countries. Today's business reality for API member companies is that they operate across borders, especially so in Information Technology (IT). And the cybersecurity threat is truly global. API advocates the further promotion and use of the Cybersecurity Framework globally so that it can serve as a baseline for policy making and for cybersecurity management for companies operating worldwide.

3. API member companies believe that the private sector should retain autonomy and the primary responsibility for protecting companies' assets against cyber-attacks.

API member companies urge the Commission and the next President to continue to grant to the private sector, which includes API member companies, the autonomy and the primary responsibility for protecting companies' networks, data, infrastructure and industrial control systems (ICS)/operational technology (OT) from cyber-attacks. This private sector autonomy has served industry well: it has incentivized significant investments, innovations and flexibility from oil and natural gas sector operators, service providers, suppliers and cybersecurity vendors to address dynamic cyber threats.

4. API member companies believe that governments should have the primary responsibility for deterring and preventing cyberattacks by nation states and organized criminal elements against the oil and natural gas industry.

API member companies believe that private sector autonomy and responsibility for the cybersecurity of its assets must be coupled with a government responsibility for deterring and preventing cyberattacks. The private sector faces the threat of cyber-attacks from a variety of actors, especially nation states, seeking to steal intellectual property and/or compromise assets such as networks, industrial control systems (ICS), etc.

As with the physical dimensions of national, economic and energy security, private sector oil and natural gas companies need to rely on the governments of the United States, its allies and international partners to deter and respond to cyber events through cyber and non-cyber methods employing all instruments of private and public power—diplomatic, economic, information, intelligence, military and law enforcement.

API supports continued US government work and investment to counter and deter international malicious actors. We support the US Chamber of Commerce Policy Statement on Cybersecurity Norms and Deterrence. API member companies would like to work closely with the new Presidential Administration to solidify work to define international norms of cyber behavior and coordinate with government efforts to deter and counter cyberattacks. API recommends greater voluntary senior-level coordination between the US government and the private sector on cybersecurity, such as yearly roundtables between the highest levels of US Government and representatives from the private sector, such as Chief Information Security Officers (CISOs) from companies.

5. API member companies support voluntary collaboration and information sharing between the private sector and government in order to protect critical infrastructure and the intellectual property of the oil and natural gas industry from cyber-attacks.

API members support information sharing and the Oil and Natural Gas Information Sharing and Analysis Center (ONG-ISAC). Companies came together through API to form the ONG-ISAC (www.ongisac.org), which is now an independent organization that shares and receives cyber threat indicators and defensive measures in real time. The center builds on existing programs to help companies quickly identify and respond to cyber threats.

API members advocated strong support for Cybersecurity Information Sharing Legislation and welcomed the passage of the Cybersecurity Act of 2015. API members recognize the value of this legal framework to govern and promote cybersecurity information sharing among and between industry peers, ISACs and the US Government.

API member companies strongly support the ongoing work of the US Department of Homeland Security to make cybersecurity information sharing operational. We recommend continued government efforts to share with the private sector cybersecurity threat indicators that are:

- Unclassified as much as possible, i.e., without attribution of sources or methods, so that they can be used by the private sector;
- Shared in real-time, machine-to-machine;
- High fidelity and actionable indicators of compromise along with additional metadata such as attack type, date first seen in relevant industry sectors (in our case, the oil and natural gas industry), extent seen in other industries, coarse infection/detection rate, etc.
- Enhanced by some classified information, shared with cleared personnel in the private sector, in order to provide additional context for companies to anticipate and address future risks.
- Shared with companies through a limited number of points of contact with government agencies to minimize duplication-and increase timely delivery of information shared.

API appreciates the opportunity to respond to the Commission's Request for Information and provide recommendations to the next President and his or her Administration.

Sincerely,

Aaron Padilla

Aaron Padilla
Senior Advisor, International Policy