energy API
AMERICAN PETROLEUM INSTITUTE

**Walter C. Retzsch**
Senior Policy Advisor - International & Cybersecurity
Tax and Accounting Policy

1220 L Street, NW
Washington, DC 20005-4070
Telephone (202) 682-8598
Fax (202) 682-8408
Cell 301-928-4132
Email retzsch@api.org

April 26, 2013

To: Office of Policy Analysis and Development
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: Incentives to Adopt Improved Cybersecurity Practices – Notice of Inquiry

The American Petroleum Institute (API) welcomes the opportunity to respond to the National Institute of Standards and Technology and National Telecommunications and Information Administration's Notice of Inquiry issued by the U.S. Department of Commerce in the Federal Register on March 28, 2013 to obtain answers to a series of questions on Incentives to Adopt Improved Cybersecurity Practices.

API is a national trade association that represents all segments of America's oil and natural gas industry. Its more than 500 members include large integrated companies, exploration and production, refining, marketing, pipeline, and marine businesses, and service and supply firms. The industry also supports 9.2 million U.S. jobs and 7.7 percent of the U.S. economy, delivers $85 million a day in revenue to our government, and, since 2000, has invested over $2 trillion in U.S. capital projects to advance all forms of energy, including alternatives.

Oil and gas industry members face various cybersecurity risks ranging from unsophisticated, unskilled opportunistic hackers to highly skilled and resourced organized crime and nation-state entities seeking monetizable information and/or destruction of valued information technology and operational technology cyber systems. Incentives are not required for oil and natural gas companies to address these cyber risks. Most companies have integrated cyber risks into their corporate risk management systems and address them like any other business risk. Although there are items (like sharing actionable information regarding threats) that can facilitate companies management of cyber risks, the oil and natural gas industry does not "require" incentives to cause us to address these risks.

The attachment to this letter provides specific answers to each of the questions posed in the Notice of Inquiry. API looks forward to working with NIST to clarify and build upon these responses to support the voluntary adoption by critical infrastructure owners and operators the Cybersecurity Framework being developed by NIST.

Should you have any questions or would like to discuss further, please feel free to contact me at (202) 682-8598 or Retzsch@api.org.

Sincerely,

Walter C. Retzsch

Walter C. Retzsch

**Responses by the American Petroleum Institute to the Notice of Inquiry on *Incentives to Adopt Improved Cybersecurity Practices***

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

  Incentives are not required for oil and natural gas companies to address cyber risks. Most companies have integrated cyber risks into their corporate risk management systems and address them like any other business risk. Although there are items (like sharing actionable information regarding threats) that can facilitate our management of cyber risks, the oil and natural gas industry does not "require" incentives to cause us to address cyber risk.

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

  As noted in response to the previous question, incentives are not required for oil and natural gas companies to address cyber risks. Most companies have integrated cyber risks into their corporate risk management systems and address them like any other business risk.

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

  Most companies consider cybersecurity as a cost of doing business. Risk scenarios are conceived and evaluated by risk assessment processes, documenting the potential impact and likelihood of an event. Most of these assessments are qualitative but some companies have begun to investigate the use of quantitative risk analysis tools to establish a quasi-return on investment on some security expenditures. Generally, return on investment calculations for cybersecurity are difficult at best and non-existent in most cases. In either case, the risk assessment results help companies prioritize which scenarios to address and which controls to implement, with focus generally on those with the highest cost/benefit relationships.

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

  Better information sharing, particularly of actionable threat indicators and finished intelligence, allows companies to focus investments on actual threats rather than spreading resources across the entire attack surface.

  Sharing industry attack information helps raise awareness that all companies, regardless of size, are potential targets.

  Subsidized training may be considered to facilitate implementation of cybersecurity practices within small business.

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

Multiple methods include incident reports and audits measure the effectiveness of cybersecurity efforts. Many companies are moving toward a maturity measure to assess programs.

Cost-effectiveness can be measured through quantitative risk analysis and most often through benchmarks of like firms.

Companies should avoid relying solely on easily obtained measures like blocked incoming attacks items (like viruses, BOTNETs, spam, spear phishing emails, etc.) as gauges of cybersecurity effectiveness as the quantity (number) of items blocked does not necessarily equate to success. No firm can determine with any certainty whether they have blocked one hundred per cent of incoming attacks and the prevention of one key attack is of much greater significant than significance than failing to stop minor nuisances.

- Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make security investments or other investments that can be applied to security?

The IT Security Subcommittee (ITSS) organized by the American Petroleum Institute (API) is a collaborative group which has influenced the way many large and small oil and natural gas companies protect, detect and respond to cyber threats. The ITSS has published several cybersecurity guidance documents and annually hosts a cybersecurity conference on behalf of the industry.

Project LOGIIC (Linking the Oil and Gas Industry to Improve Cybersecurity) is a public/private partnership that leverages US Federal and oil and natural gas industry resources to execute cybersecurity projects to develop solutions to protect critical infrastructure. LOGIIC provides an "incentive" of testing possible implementations, obviating companies of the time and cost of developing similar solutions.

The DHS Cyber Information Sharing and Collaboration Program (CISCP) program provides incentive to participating groups/companies by facilitating acquisition of clearances at the secret and/or top secret level.

There are other organizations like the Cybersecurity Working Group (CSWG) that serves as the subject matter expert body to the Oil and Natural Gas Sector Coordinating Council (ONG SCC). The efforts of the CSWG are designed to create an educational message for the oil and natural gas sector to increase their understanding of cybersecurity. The CSWG also works in close collaboration with the pipeline, chemical and electricity sectors on cybersecurity initiatives, as well as working with the Department of Energy, Department of Homeland Security, and other government agencies.

- Are there disincentives or barriers that inhibit cybersecurity investments by firms? Are there specific investment challenges encountered by small businesses and/or multinational companies, respectively? If so, what are the disincentives, barriers or challenges and what should be done to eliminate them?

Multi-national firms face multiple and sometimes contradictory regulatory regimes that can inhibit implementation of certain security controls. Monitoring is a key example which is easily implemented within the US but requires evaluation and justification elsewhere to ensure compliance with privacy and other regulation in other jurisdictions. Log management is another; some countries consider basic networking elements as Internet Protocol address as personal information and consequently restrict transfer of this data across national boundaries. This can prevent collating log data across the

company and preclude "Big Data" analytics from locating anomalies which may be precursors or evidence of attacks in progress.

Small businesses often face the challenge of having sufficient funds to implement all the defense-in-depth security tools and operational support required to effectively protect against, detect and respond to cyber threats. In addition, the initial investment is often short lived as bad actors adjust their tactics and relentlessly look for weak links to exploit.

Some companies may not consider themselves to be a specific cybersecurity target; however, the company may still be targeted as part of "supply chain" attacks as a means to access and/or attack larger business partners.

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

Often, incentives are more impactful on small business than on large companies. The impact that cyber threats has on smaller companies is often much harder to quantify and bring to the businesses bottom line.

Sharing industry attack information helps raise awareness that all companies, regardless of size, are potential targets.

Government technical assistance and training may facilitate implementation of cybersecurity practices within small business.

- 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?

Compliance and security might be considered to be opposite ends of the same spectrum. Compliance might be defined as ensuring proper controls are in place and operational. As such, compliance is often "backward" looking as one generally has to have experienced incidents/attacks to be able to design and assess the effectiveness of controls. Measuring compliance is often more burdensome and costly than implementing the actual controls. FISMA is a good example because the costs of proving compliance were significantly higher than the cost of implementing the protections.

Compliance is a necessary component of overall cybersecurity but too much emphasis on compliance (that is, addressing experienced, known attacks) leaves a corporation vulnerable to new, different attacks which may not have previously been seen. Prescriptive regulations mandating use of specific controls can be detrimental; the controls mandated by regulation may no longer be the most appropriate and resources used to implement these controls to meet the compliance requirements are resources which are unavailable to implement controls more effective against contemporary threats. Most experts within the cybersecurity industry will universally state that compliance is not security.

Cybersecurity needs to incorporate compliance (as old threats never die nor do they fade away) but balance it with other (detection/containment) controls that can manage futuristic threats/attacks as well as the known/old.

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

Much of the business community considers liability protections to be one of the more favorable incentives. That said, this benefit would have to be balanced against the means by which one proves adherence to the program; the prospects of submitting to third party or government audits periodically might offset the benefits of the legal safe-harbors.

Measuring cybersecurity is always a difficult proposition. Reliance on audits can create a compliance culture that, as stated in the answer to the previous question, is backward looking and does not truly engender security. The final result of such a program for critical infrastructure is a false sense of security with companies complying with the DHS program but still suffering from cyber attacks that affect critical infrastructure.

There is also difficulty in assessing what "reasonable care" entails.

- What would be the impact of requiring entities to join the DHS Program prior to receiving government financial guarantees or assistance in relevant sectors?

The impact may be muted as the industry, when evaluating the 14 broad categories of potential incentives, viewed tax incentives (i.e., tax credits and/or deductions) more favorably than grants.

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

This is another area where the industry is split. Many oil and natural gas companies are sufficiently large that they self-insure and consequently are not interested in external insurance coverage. Liability considerations, though, are of interest to many in the industry.

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

This is part of doing business in the twenty-first century. Companies that do well with cybersecurity will have fewer attacks/problems and will be more efficient with their operations which will result in more profits.

The situation is similar to safety; companies with poor safety records have historically fared worse than industry competitors with better safety records. Poor cybersecurity practices can affect the bottom line and this is the best market tool/force available.

- 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?

The Framework should be published (like any other NIST document) allowing companies to use it in total, adapt it, or select specific portions for internal use. Most companies already have their own internal cybersecurity frameworks or alternatively use international standards (e.g., ISO 27000); some countries require use of specific standards. Companies are unlikely to be able to eschew these existing frameworks for a new one and, consequently, the Framework needs to be able to fit within existing environments.

The Federal government should first implement an awareness program that spells out why this Framework is being provided and what is in it for small businesses, which may not otherwise understand. Next, the government should assist any company that asks for help with implementation

to put the guidance in place. For multinationals, the ability to implement consistent practices on a worldwide basis is a key to adoption and the government must work with international standard bodies and with various governments to assure that laws, regulations, and standards around the world will work appropriately with the standards that the U.S. government / NIST releases.

- 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?

  All companies within these industries must be made aware of new suggested practices, implying a need of a Federal awareness/communication program.

- 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?

  Actionable, timely information sharing is the best means to ensure that companies are aware of the latest threats and can adjust their threat detection and mitigation measures accordingly.

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.

- Do organizations participate in voluntary governance mechanisms?

  We interpret voluntary industry sector governance mechanisms to mean standards settting organizations. API manages a voluntary standards development program for the oil and natural gas industry. API standards, recommended practices and guidance documents are voluntary, but often become best practices for the industry. API standards are used both domestically and internationally.

  Which industries/groups have voluntary governance mechanisms?

  See preceding response.

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

  API has cybersecurity-related standards and guidance documents. A new guidance document related to operational technology (i.e., ICS, PCS, SCADA, etc.) is under development. The API Information Technology Security Subcommittee has developed other cybersecurity guidance documents that are available to API members.

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

  API standards are designed to assist industry professionals improve the efficiency and cost-effectiveness of their operations, comply with legislative and regulatory requirements, safeguard health, and protect the environment. Each year, API works with leading industry subject-matter experts to maintain an inventory of over 600 standards and recommended practices. API distributes over 250,000 documents annually worldwide, and continues to strive to enhance safety operations,

improve quality assurance, and promote the global acceptance of petroleum products and best practices.