AMERICAN PETROLEUM INSTITUTE

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

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

April 8, 2013

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

Re: "Developing a Framework to Improve Critical Infrastructure Cybersecurity."

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 February 26, 2013, to assist in defining the voluntary cybersecurity framework ("Framework") required by the February 12, 2013 Presidential Executive Order entitled "*Improving Critical Infrastructure Cybersecurity*".

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 threat actors ranging from unsophisticated, unskilled opportunists to highly skilled and resourced organized crime and nation-state entities seeking monetizable information and/or destruction of valued systems. The developed Framework must address these different threats and, as capabilities vary significantly; simplistic one-size-fits-all approaches will not likely succeed. The Framework must be flexible to include traditional defenses and moving target defenses, sharing indicators of compromise and anomaly detection/incident response to handle more nefarious adversaries.

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) 682-8598 or Retzsch@api.org.

Sincerely,

Walter C. Retzsch

American Petroleum Institute Response to National Institute of Standards and Technology (NIST) Framework for Reducing Cyber Risks to Critical Infrastructure Request for Information (RFI)

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?

We consider the following items as the greatest challenges in improving cybersecurity.

1. Suppliers do not provide "Secure by Design" products. This is particularly true in process control environments where vendors have not certified their systems for various cybersecurity tools that would greatly improve our security posture.

2. Technologies, threats, demographics, regulation, and business models are evolving at a quicker pace than some can accommodate.

3. Critical infrastructure by definition is very broad and each sector will have different hardware, software, and process requirements. Huge legacy infrastructure may become vulnerable because of changing threats and connectivity.

4. Another challenge is the lack or misallocation of resources (i.e., people and technology). Most resources currently are focused on prevention but we need to move more to a detect/contain model. Critical infrastructure organizations should be provided a set of objectives that can reduce the chances of infection, help identify already infected machines, and then provide assistance in carrying out their objectives in the form of information sharing, training and technical assistance.

5. Finding common ground for business, IT, and government (lawmakers) to discuss security issues and share actionable threat information. Legal indemnity would facilitate this information sharing.

6. Cyber adversaries constantly change attack methodologies and tools so a compliance regime mandating specific controls across all critical infrastructures to manage threats and risks is doomed to fail as it precludes critical infrastructure providers from changing their practices quickly enough to address rapidly changing threats. Such mandatory, static controls would also make it simple for cyber adversaries to avoid the controls. An example of this is the use of Virus Total by so called APT attackers...They can quickly

check to see if any current anti-virus program will alert on their attack code before sending it.

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

All critical infrastructure sectors likely use an "office environment" (i.e., business network) in which they conduct daily business operations. This part of their network provides office tools such as email, word processing, spreadsheets, accounting, and HR functions. A framework of control objectives for the office environment could probably be used across all critical infrastructure segments if it were sufficiently generalized and help organizations that may be lagging behind.

There is some concern that a least common denominator approach may negatively impact those on the leading edge. Standards for core elements must be clear and there must be sufficient clarity to address differences between sectors, within sectors and within company businesses.

Each sector, though, has different key assets that will be prioritized and protected differently. Reaching a decision within the Framework on taxonomy and severity of risks will be a challenge.

Even within a sector, there will be variation. Tools used to run a pipeline will differ from those used to run a power plant, which differ from those used to run a refinery. 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. Control objectives will be largely consistent across these segments, but the controls will vary significantly.

A key aspect of any attempt to standardize controls across all sectors (or even across a single sector that includes a broad range of operations, such as the oil and gas sector) is that many corporations operate critical infrastructure across multiple segments and/or across multiple countries. Mandating particular controls in segment A and different controls in segment B will prevent such organizations from looking across their environment for synergies (i.e., places where they can use common controls to meet their control objectives in multiple segments or to meet potentially differing requirements of multiple countries).

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?

Industry companies generally have a risk based corporate level security framework that outlines general principles (e.g., information security is commensurate with risk and business value) and management responsibilities. These broad policies are supplemented by more specific standards, technical controls, and guidance that assist individual business units in assessing their risk and selecting appropriate controls. Cybersecurity is integrated into corporate risk management processes and business units must report deficiencies and provide mitigation plans to senior management. Senior management is also apprised of key risks and remediation efforts periodically.

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

Industry companies generally house cybersecurity risk management within Information Technology. Corporate risk management and/or physical/global security organizations may also have some shared responsibility.

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

Risk is generally defined as a function of threat, vulnerability, likelihood, consequence and mitigating controls. The latter may prevent, detect, or contain the risk.

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. The overall risks of cyber attacks are looked at together so that it is possible to identify gaps between the controls implemented by individual application or technology owners.

Both qualitative and quantitative means are used to assess risk. For each business, separate risk and control teams work with information owners to identify risks. Quantitative analysis is targeted toward strategic/key risks reported to senior management. A significant effort is made to evaluate the cyber risk environment by sharing information with industry groups, computing advisory firms, and various government entities. In addition to sharing general information, particular attacks have led some corporations to provide more detailed attack information on certain types of attacks to government entities.

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

Most industry firms have completely integrated cybersecurity risk into their company's overarching enterprise risk management systems.

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

Industry members use a variety of different frameworks including COBIT, COSO, ITIL; as well as other standards, tools and good industry practices, such as API, SANS, ISO, FERC, NIST, ISF, FAIR, Australia DoD standards, and ISA. Many companies use home-grown, company developed tools that may resemble ISO 17799/27002 or COBIT, but which pre-date these significantly. Some companies may also use a GRC to contain policy and controls, risk statements and compliance assessments.

Several companies use an annual representation process in which each level of management asserts to the board that they are in compliance with standards and required practices and detail any outstanding items. These risk assessment and mitigation processes have been continually improved over the years. Benchmarking has also been 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 industry members include (but are not restricted to):

1. SOX;
2. SEC cyber risk reporting guidance;
3. CFATS;
4. NERC/FERC CIP (for joint venture power plants/utilities);
5. TSA (Pipeline);
6. HIPAA;
7. State Data Breach Notifications;
8. Non-US privacy law (EU, Canada, Singapore, China, Argentina, and others);
9. Payment Card Industry (PCI) standards; and
10. Various requirements for drilling, producing, transporting, refining, packaging, and selling petroleum and natural gas based products.

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

Corporations have a wide range of assets and processes that may be considered critical under some definitions. Many of these are dependent on externally provided services such as power, water, telecommunications (such as data transfer via satellites or local microwave from an offshore rig to a service provider), financial services, and transportation. In addition, many of them could depend on internally provided services in these same areas. Business continuity plans and disaster recovery plans are developed as needed to address interruptions in key services and to mitigate their risks.

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

Health, environment, safety, security, reliability and resiliency are principal performance goals. It should be noted that physical security plays a key role in protecting cyber assets, and that physical security programs need to be integrated with cybersecurity programs. Many cybersecurity measures can be compromised if basic physical security measures are not in place; for example, access control to software and hardware, and employee and contractor background investigations are essential to comprehensive security programs.

Corporations use a variety of service-level objectives that encompass the idea of restoring services within appropriate timeframes. In the case of cybersecurity events, the service level for users performing critical services will not normally be impacted due to attackers being stopped prior to disruption of services. However, cybersecurity events could potentially impact enough devices to disrupt services and plans have been developed to address such events. These plans will differ based upon the nature and scope of the attack and the degree to which the initial attack was successful. In the case of critical infrastructure devices that may control process control systems or distributed control systems, the business unit will usually have safety and security plans in place. Should general purpose business computing systems be attacked and destroyed or disrupted, plans are typically in place for mass reload of such machines.

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?

Many industry members are subject to multiple US Federal regulatory bodies including SEC, NERC/FERC, DHS, TSA, USCG and DOT among others. Companies may also need to report to state/provincial and non-US Federal bodies depending upon incident (a data privacy breach, for example, would require notification of various state agencies) and location of business.

Reporting requirements differ for the different segments of companies. Some reporting has been straight-forward and reasonably efficient. Other reporting is more difficult and time consuming and in many cases it does not appear to have any security value.

A formal government program to classify sensitive information and to provide protection from discovery in civil litigation or disclosure under the Freedom of Information Act (FOIA) is essential if organizations are expected to share and report sensitive proprietary information. A program similar to the DHS Chemical-terrorism Vulnerability Information (CVI) Program or the DOT Security Sensitive Information (SSI) Program could serve as a model.

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

Standards provide companies a means to address general security requirements; however, none by themselves are sufficiently comprehensive to cover all security requirements. The standards creation/update process is slow enough that the standards organizations alone cannot handle rapid changes in threats, technology, etc.

International standards organizations help provide a consistent taxonomy across the globe.

Corporations should document the standards that they intend to use in the area of cybersecurity whether they elect to use a framework such as ISO 27000 or COBIT or develop their standards internally. They should then perform periodic audits of their compliance with their adopted standard(s). These audits could be performed by external assessors or by appropriately independent internal assessors.

Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, 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 seeks comments on the applicability of existing publications to address cybersecurity needs, including, but not limited to the documents developed by: international standards organizations; U.S. Government Agencies and organizations; State regulators or Public Utility Commissions; Industry and industry associations; other Governments, and non-profits and other non-government organizations.

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. Please provide information related to the following:

1. What additional approaches already exist?

Industry members use a variety of different standards including (but not restricted to) ISO 27000, ISA 99, TSA Pipeline Standard, PCI, NERC/FERC CIP, NIST, HIPAA, GLBA, API 1164, SANS Top 20, and Australian Top 35.

Some members only use these standards to meet compliance requirements; in some cases, members have mapped their home-grown, company developed standards to (some of) these different regimes.

2. Which of these approaches apply across sectors?

General purpose frameworks such as ISO 27000, COBIT, NIST, ISF, and SANS Top 20 controls apply across all sectors to the extent that they all have business networks / office environments. Should organizations adopt one or more of these as their framework, they could use it to manage the business networks across all of their critical infrastructure business areas.

Other standards apply across sectors in specific cases. Payment Card Industry (PCI) standards apply to any sector that processes credit cards. ISA 99 will apply to any sector with process control systems.

Regulatory regimes, like HIPAA and GLBA, will apply across sectors, but to subsets of companies dealing with health and financial information, respectively.

3. Which organizations use these approaches?

The general standards like ISO and COBIT can be used by any company. ISF likewise fits in this category but use is restricted to ISF members. ISA is used by companies with control systems. The TSA pipeline standards are used by pipeline firms. The PCI standards are used by companies that accept credit cards. NERC/FERC covers primarily utilities, but the regulations extend to any facility capable of placing certain amounts of electric power on the national grid.

HIPAA pertains to health data and GLBA to finance; any company providing health care or insurance or dealing with financial institutions is likely going to have to contend with these standards/regulations.

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

Many are focused on specific environments and/or have specific goals. Even the most general do not cover everything and, therefore, must be customized or extended by individual companies. Some allow a good deal of variation based on company tolerance of risk while others tend to be more prescriptive, requiring specific controls. All are relatively "static" because the time needed to change or amend such standards is slow in comparison to the pace of changes for technologies, threats, and the like.

These frameworks tend to focus primarily on preventive controls and therefore are generally effective only against moderate or low skilled adversaries. Information/intelligence sharing to enable better detection capabilities and incident response to contain the infiltration are needed to address higher skilled adversaries.

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

Harmonization of the approaches would be helpful, particularly if one has to contend with compliance to multiple regimes. Flexibility and reality are two other elements; some tend to extend their scope to any potentially accessible system even if there are controls that limit or preclude direct network connection. Organizations should be able to adopt a standard and then make appropriate modifications to the standard to fit with their business environment. Once they have adopted "their" standard(s), companies should periodically review compliance to those standards via external audits, internal audits, or other reviews by parties independent of the group responsible for execution of cyber security.

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

API 1164 is perhaps the most specific, covering liquid pipelines. The other approaches generally do not take into account sector-specific needs. ISO bases control selection on a risk assessment conducted by the implementer; the implementer could then insert its own sector-specific elements within this area. Broad frameworks such as ISO 27000 and COBIT can allow enough flexibility to allow them to be used across multiple segments while allowing the business to define the sector-specific controls that the need.

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

New sector-specific standards developments are not needed unless or until gaps arising from new threats and risks have been identified, at which time the standard development process can be initiated.

All standards have positives and negatives and use should be voluntary, not mandatory. The oil and gas sector has so many variations of companies (large/small, US only/international, integrated/focused on one industry area, service company/oil) that a single standard will not likely suffice. Oil and gas sites can also be subject to multiple sectors (e.g., chemicals, utilities) and under jurisdiction of multiple regulatory regimes both in the US and abroad. It would be better to allow selection of appropriate standards/controls based on company risk assessments and risk management decisions, than to force a company to have to implement multiple mandatory requirements.

Each business should be allowed to determine how it will meet the cybersecurity objectives of whatever 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?

Sector-specific agencies and related sector coordinating councils can be very helpful in assuring that all companies within a sector understand the threats and potential controls / approaches in their sector. In some sectors, companies may wish to have standard industry practices developed on behalf of the segment, whereas others may wish to keep this at the company level with coordination and guidance from the agency / councils.

Across sectors, sector-specific agencies and sector coordinating councils should work cooperatively through the Partnership for Critical Infrastructure Security (PCIS) to assist NIST in developing standards, to advise agencies on implementation, to help manage the harmonization of different approaches, and perhaps to provide assistance to smaller companies who may be resource constrained. As the principal cross-sector advisory group to the US Government, the PCIS can add significant value to the process. The agencies and councils should consider co-sponsoring events or forums to help share knowledge and direction across sectors.

9. What other outreach efforts would be helpful?

Outreach efforts that may be helpful include:

- Emphasis on bi-directional, secure, and anomymized communication between companies and government;
- Ask that the management of each corporation attest that they are meeting the cybersecurity objectives required for the critical infrastructure segments in which they operate;
- Good material on user education and awareness;
- Scrubbing of the internet (i.e., earlier identification and removal of malware);
- Ensuring that there is sufficient supply of skilled staff; and/or

- Development of materials on how to improve resilience and robustness of infrastructure.

Specific 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?

The listed specific industry practices are generally implemented in the corporations in our industry. We believe that they are all used broadly, but not universally and at differing maturity levels within the oil and gas industry.

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

Industry members operate in many countries around the world 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. For instance, European privacy standards can restrict/inhibit monitoring, and impact our ability to adequately protect data from theft. It is recommended that any proposed U.S. standards be discussed with international standard bodies (e.g., the EU Cybersecurity Directive) and vice versa.

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

The most critical practices are:

- Separation of business from operations systems;
- Identification and authorization of users access systems;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures; and
- Asset identification and management.

Providing at least some separation between control and office systems is a well-known, common industry practice and can keep a production network operational should the office network be compromised. (See the Shamoon attack on Saudi Aramco as an example.) Standard identification and authorization is a primary control to protect resources. As we have to expect to be compromised at some point, detection via monitoring and containment via incident response become key tools to manage an attack and restore/maintain service. Knowing what resources (assets) one has and where they are located is another key practice.

Not listed, but also critical, is having informed, well-trained personnel utilizing each of these.

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

Not all of these practices are applicable in every situation.

Even within a segment, certain technologies such as encryption should not be used on all communications. It may also not be appropriate to expect privacy protection for data on a process control system. For certain process control systems, having authentication requirements such as password protected screen savers can become a safety issue, potentially delaying resolution of an issue and making it worse.

Asset identification and management is traditionally considered critical but the proliferation of consumer end points owned by different people/organizations may make this less of a requirement in the near future (and engender an architecture where the end point is never trusted.)

Security engineering and resiliency practices are nice, but one can make do with monitoring/incident handling if need be.

Monitoring tools that are used in business environments may not be appropriate in a process control environment.

Incident handling processes may be superseded by safety processes in some environments. This should be recognized in any standards developed.

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

Many of these practices have challenges. It is not possible to totally separate business and operational systems due to the nature of running a business. Therefore, any ability to connect these systems must be scrutinized closely and managed on an ongoing basis.

Encryption can be easy to manage if it is done as full disk encryption on every end-point device on the business network. However, this does not really provide an effective control against a cyber attacker that compromises a PC and installs a remote access Trojan on it. Managing multiple encryption regimes within an external collaboration environment is extremely complex if not impossible at times.

Asset identification has historically been a difficult problem but architectures that do not "trust" end points may make fixing this problem moot.

Monitoring requires hardware and personnel, both of which may not be available. Even if present, large networks will generate huge swaths of data that must be perused with (Big Data) analytics. Input from the business regarding key assets and "normal" operations is needed to help identify anomalies; the business, though, may not actually understand its own processes to this detail. Most companies are not particularly mature in this area, nor is the technology necessarily mature either.

Identity and access management is typically managed in silos (i.e., per system/application) and lacks a central, overall viewpoint. This can lead to privilege creep, because it is difficult to ascertain just what a particular user can access, or improperly protected data, because it is too difficult to manage access lists for large user populations.

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

Standards/guidelines provide a solid minimum baseline of security.

Regarding the specific practices, separation of business and operations networks is a key tenet of ISA 99. Privacy compliance most often follows the most restrictive regulatory regime to which the company is subject.

Many of the other practices are covered in general standards like ISO 27001 although implementation details must be selected/handled by individual companies.

Some have implemented full disk encryption and use additional encryption or rights management on certain storage areas. Very little of this encryption is designed to protect computers that manage control systems.

Some have detailed guidance on authorization and authentication, and perform reviews on use of certain privileged accounts.

Most have asset management systems with associated processes.

Companies have implemented a wide variety of monitoring and incident detection tools and capabilities. These include both commercial products and in-house developed products. Practices for these various tools have been defined.

Incidents are generally managed with a commercially available incident management system along with incident management practices and procedures that were internally developed.

Resiliency practices have been defined for critical systems in both business continuity plans and in disaster recovery plans for critical systems.

The architecture of our security has been defined through internal processes and uses a security in depth model with enhanced detection and remediation processes.

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

Many companies use a budgeting model that allows business organizations to manage their IT investments. However, the IT organization also has a separate budget that allows it to assure that security related issues are addressed in addition to reliability and efficiency objectives.

Others are less efficient, using less than optimal cross-functional efforts to manage resources.

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

Formal processes exist to triage alerts / incidents and escalate those as required. We would escalate ones that changed from attempts to actual compromises and escalate further if there were a data extraction or destruction of company data/computing resources.

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

There needs to be a balance between privacy and monitoring.

Monitoring can often be done by computer systems that do not present any personal data to humans and should not be considered a risk to privacy or civil liberties. However, in some cases, content must be analyzed by humans where data that are subject to privacy requirements could be viewed. We must exercise care to distinguish user generated content from executable code in our guidance since reviews of executable code should not be considered a privacy issue, whereas review of user generated content may be.

Avoiding the monitoring of personal data is not possible if a company allows bring-your-own-device to work. Marking something as personal to exempt it from monitoring provides a convenient path for an attacker to hide. Rules treating IP addresses and/or log data as personal information (and thereby banning export) prevent collating events across an entire company.

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

The Framework needs to be flexible enough to be implementable worldwide, if so desired. Corporate networks extend around the world and companies cannot have one security model in one part and another elsewhere. Operations are extended across the entire network so creating "stronger" protections around one country alone (e.g., the U.S.) is not going to provide adequate protection. If we cannot use a consistent set of tools and practices globally, we will be hindered or impeded from efficiently securing our corporation. Every requirement that designates specific tools and/or practices (as opposed to goals/objectives) runs the risk of conflicting with mandates from some other country. This can potentially make our corporations and our nation significantly less secure. The U.S. government should work with the global community to assure that our cyber requirements allow companies to operate in a global environment without being impeded by poorly thought out mandates.

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

The U.S. government should work with the global community to assure that our cyber requirements allow companies to operate in a global environment without being impeded by poorly thought out mandates.

Privacy and security need to be balanced. Monitoring is required to protect one's network but one must not use this information to unnecessarily spy on individuals. There must be grounds or reasonable suspicion to monitor individuals. Alternatively, we cannot bend so far toward the privacy sphere that it becomes impossible to adequately monitor/protect systems and networks. Risk assessments and/or contract review with vendors should include reference to applicable laws, and should be reviewed for privacy implications. A middle ground must be found that allows actions to defend networks while not trampling individual rights.

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

Traditional legacy defenses, like firewalls and anti-virus, are not by themselves sufficient to address contemporary threats but they can effectively address older threats and should be included in the Framework.

Vulnerability management is a key to reducing the attach surface in an environment. All corporations should review current vulnerabilities and available patches and determine whether they should make changes. It is not always reasonable to install all patches, so that should not be mandated.

Threat intelligence/situational awareness seems to be a newer service that most companies are implementing to try and characterize and understand threats better. Corporations should be encouraged to share indicators of attack and indicators of compromise with others. This could be done through a program such as the U.S. government's CISCP program or through segment specific sharing efforts.

The human element needs to be considered as humans are often targeted by phishing attacks and become a first and last line of defense. Corporations should attempt to make their employees aware of the current threat landscape and encourage them to take reasonable precautions. Most companies provide some type of awareness training via traditional class room/CBT but this material should be supplemented by other aspects (like phishing exercises) and means (like "Tweeting"). The effectiveness of the training, and not just how many people took it, must be measured. Knowledge, though, is but one aspect of the human element; one must also address human ability, motivation, and triggers to follow through with action.

Legislation might be considered to force security by design, in conjunction with incentives like tax breaks.