NIST RFI-Cyber Framework – Berkshire Hathaway Energy Comments
10.8.14

REQUEST FOR INFORMATION
The following questions cover the major areas about which NIST seeks comment. They are not intended to limit the topics that may be addressed. Responses may include any topic believed to have implications for the degree of awareness and voluntary use and subsequent improvement of the Framework, regardless of whether the topic is included in this document.
While the Framework and associated outreach activities by NIST have focused on critical infrastructure, given the broad diversity of sectors that may include parts of critical infrastructure and the intention to continue to involve a broad set of stakeholders in use and evolution of the Framework, the RFI generally uses the broader term "organizations" in seeking information. NIST is especially interested in comments that will help to determine the Framework's usefulness and potential applicability across all critical infrastructure sectors. In addition, considering the interwoven nature of our Internet-based economy and society, information from and about organizations not included in critical infrastructure sectors also will be valuable.
Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Do not include in comments or otherwise submit proprietary or confidential information, as all comments received in response to this RFI will be made available publically at http://www.nist.gov/cyberframework/cybersecurity-framework-rfi.cfm.

Current Awareness of the Cybersecurity Framework
Recognizing the critical importance of widespread voluntary usage of the Framework in order to achieve the goals of the Executive Order, and that usage initially depends upon awareness; NIST solicits information about awareness of the Framework and its intended uses among organizations.

Section 1 for reference

1.

a) What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations?

- In the energy sector, and more specifically, among electric utilities, organizations with assets that are part of the bulk electrical system (BES) largely have a high level of awareness regarding the existence of the NIST Cybersecurity Framework.

b) Six months after the Framework was issued, has it gained the traction needed to be a factor in how organizations manage cyber risks in the Nation's critical infrastructure?

- In the energy sector it has. The complimentary nature of the Cybersecurity Framework and the Department of Energy's Cybersecurity Capabilities Maturity Model, reduces the burden for many energy sector organizations to make progress in Framework utilization,
- Berkshire Hathaway Energy identified further enhancing cybersecurity incident response as a priority prior to the development or release of the NIST

Cybersecurity Framework. In this way, the framework has been used internally in validating and visualizing cybersecurity projects.

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

- National Institute of Standards and Technology
- Department of Energy and recommended use of the Electricity Subsector Cybersecurity Capability Maturity Model to assist in Framework adoption
- The Cybersecurity Framework was a frequent topic of conversation at the DOE Cybersecurity for Energy Delivery Systems Roadmap Milestone: Peer Review & Assessment in Washington D.C. (August 4 – 9, 2014)

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

- Participation in industry group meetings with Edison Electric Institute and American Gas Association to discuss the application of the Framework and lessons learned.
- Berkshire Hathaway Energy business engaged in several events in 2013-2014 as part of *Safeguard Iowa* through Iowa Department of Homeland Security & Emergency Management and the National Domestic Preparedness Consortium. A broad understanding and application of publically-available cybersecurity standards and guidelines facilitated information sharing with government and private-sector customers.
- Safeguard Iowa events focused on framing issues within the context of the *Community Cybersecurity Maturity Model*. Framework usage and familiarity assisted in preparing company attendees to communicate holistic cybersecurity best practices and company approaches to risk management.
- Responding to a request made during the Safeguard Iowa Cyber Exercise, the businesses shared the framework with a local government information technology staff. The Electricity Subsector Cybersecurity Capability Maturity Model and the NIST 800 series were also shared along with examples on how they are utilized in the energy sector.

4. Is there general awareness that the Framework:

a. Is intended for voluntary use?

- Largely. We are supportive of the Framework's voluntary nature as the energy sector already has mandatory standards to meet in this capacity. The framework has been found to be more valuable as a voluntary program used to augment an existing focus on cybersecurity best practices and to seize opportunities for industry leadership.

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

- No, this is primarily known only to those who have worked closely with it and are engaged in organizational adoption in some capacity.
    - Many people still see the framework as a list of recommendations (more prescriptive) rather than a compilation of practices and policies that need to be assessed and interpreted with an appreciation of the unique characteristics and priorities of their sector and organization.

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

- Yes, references (NIST 800 series, ISO 2700x, COBIT, CCS CSC) are mapped in the Framework document. Anyone who has reviewed the Framework in detail certainly has an appreciation that they are part and parcel of the Cybersecurity Framework.

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

- Sectors that have not already defined sector specific guidance and a common approach to adoption will likely pose challenges.

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

- The financial sector is likely to have far greater visibility on this question

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

- The regulator stakeholders with the lowest level of awareness likely sits at the state level, such as public utility commissions. That said, numerous regulator agencies have expressed an interest and awareness of the Framework.

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

- As mentioned in response to question three, engagement with customers and other utilities presented several opportunities for outreach and education.

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

- Supplier education and awareness to ensure alignment between offerings from suppliers and the needs of critical infrastructure organizations. This supplier engagement issue has been an industry goal and an issue that government participation supports, including through venues such as the Roadmap to Achieve Energy Delivery Systems Cybersecurity sponsored by the Department of Energy.

Experiences with the Cybersecurity Framework – **Section 2 for reference**

NIST is seeking information on the experiences with, including but not limited to early implementation and usage of, the Framework throughout the Nation's critical infrastructure. NIST seeks information from and about organizations that have had direct experience with the Framework. Please provide information related to the following:

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

- The Framework has done more to help the public understand the importance of managing cyber risk.
- An appreciation for the importance of managing cyber risk had been identified by electric utilities before the Framework came to pass.

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

- The Energy sector is using the Framework through application of Electricity Subsector Cybersecurity Capability Maturity Model
- The Electricity Subsector Cybersecurity Capability Maturity Model toolkit has been used to conduct a high level assessment of cybersecurity risk management maturity and analyze current and planned projects to be used for consideration in project selection.

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

- Covered within other sections

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

- The thorough mapping to other standards/guidelines is helpful and provides an idea of what the framework hits vs. what is out there or being done already.

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

- Organizations in all sectors require some level of sector specific guidance prior to use. That guidance can and should be self-developed within the sector.

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

- Yes, the Framework has been utilized and integrated within its broader enterprise cyber risk management program.

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

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

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

- In very early stages, if organizations already track to ISO, PCI, COBIT, FISMA, the logical first step is to compare that posture to the components of these standards that are used and noted in the framework

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

- The Framework has been integrated into a developing metrics and benchmarking program.
- The Framework is used amongst other standards, guidelines, and benchmarking efforts to drive future planning and in maximizing return on investment in cybersecurity control projects

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

- No comments.

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

- No comments.

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

- We use the framework as a reference for stakeholders such as state commissions, internal executives and insurance underwriters.

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

- Yes, relative to use of the associated Energy Sector Control Systems Working Group's (ESCSWG) "Cybersecurity Procurement Language for Energy Delivery Systems" (April 2014) in defining enhanced cybersecurity requirements to suppliers and other third parties.

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

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

- Covered in Q2 in Section 2

Roadmap for the Future of the Cybersecurity Framework - **Section 3 for reference**

NIST published a Roadmap in February 2014 detailing some issues and challenges that should be addressed in order to improve future versions of the Framework. Information is sought to answer the following questions:

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

- It does at a high level; although, it should be noted that the areas are discussed broadly and are not prioritized within the confines of the roadmap. An activity which likely needs to be identified at the critical infrastructure sector and organizational level.

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

- These are likely to be sector specific .
- A potential issue that may warrant consideration or inclusion within an already identified category is: malicious cyber-device identification in physical security assessments and incident responses.
    - Thinking here of devices similar to commercial devices available like Pwnie Express, Pwn Plug (R2, Elite), Rubber Duckies, Ominous Box for WiFi Pineapple, LAN taps, etc.
- Within the energy sector, appreciating that the roadmap identifies issues and opportunities at a *very* high level; it may be observed that Authentication (4.1), Conformity Assessment (4.3), Supply Chain Risk Management (4.8) and to some degree Automated Indicator Sharing (4.2) [although the degree to which the process is automated is not a foremost concern] are areas of increased emphasis and attention.

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