Duke Energy responses to NIST Cybersecurity Framework RFI – 10/6/14
Prepared by: Ed Goff, edwin.goff@duke-energy.com, 919-215-8856

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.

1. What is the extent of awareness of the Framework among the Nation's critical infrastructure organizations? 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?

> *Duke Energy is fully aware of the Framework. Improved risk management practices are being implemented and an enterprise implementation of ES-C2M2 is planned.*

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?

> *Duke Energy has been engaged in the process from the initial workshop through to the development of the implementation guidance. Our close, valued relationships with DOE, NIST and various industry associations like EEI, AGA, UTC, etc. keep us well informed.*

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?

> *Yes. Duke Energy actively participates with DOE, EEI, AGA, UTC and others in the adoption of the Framework. Additionally, Duke Energy is sharing ES-C2M2 data with our utility peers which is fostering lessons learned as it relates to Framework adoption.*

4. Is there general awareness that the Framework:

> a. Is intended for voluntary use?
>
> > *Yes.*
>
> 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?
>
> > *Yes. The Framework is used in justification of business cases for ES-C2M2 adoption and improved risk management practices.*

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

Yes. We will use the mapping to ES-C2M2 from DOE and other tools we were already using e.g. NIST 800 series standards, NERC CIP, etc.

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?

Duke Energy sees no challenges to improving awareness of the Framework in the private sector. Existing approaches with our SSA, industry associations and critical infrastructure protection committees seem adequate.

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?

We are using the Framework and ES-C2M2 for our overall cybersecurity program that encompasses our international operations. Many suppliers we deal with are international and are engaged in use of the Framework.

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?

Yes. There have been references to the EO and the Framework in NERC & FERC meetings.

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?

Yes. We are communicating with internal stakeholders and we have presented at numerous EEI Security Committee and SANS SCADA Summit meetings on the development of and implementation of the Framework using ES-C2M2.

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

Awareness is adequate in our opinion.

Experiences With the Cybersecurity Framework

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.

Duke Energy responses to NIST Cybersecurity Framework RFI – 10/6/14

Prepared by: Ed Goff, edwin.goff@duke-energy.com, 919-215-8856

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?

> *Yes. As the Framework was being developed, the key message from the first workshop in Washington, DC was the expectation of more mature and comprehensive risk management. Out of that initial workshop, we began overhauling our risk management program.*

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

> *For the Framework, Duke Energy is primarily engaged with the Energy Sector. We are also tracking Nuclear, Chemical, Transportation & Dams sectors to ensure our approach with ES-C2M2 meets expectations. Duke Energy has been actively engaged with DOE and other agencies in the development of our sectors implementation guidance document.*

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

> *The ability to use existing tools like the ES-C2M2 to implement the Framework. The Framework has helped with a common understanding of cybersecurity risks and how that helps business cases needed to realize more mature capabilities/security posture.*

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?

> *None. The most helpful is the ability to use existing tools like the ES-C2M2 to implement the Framework because we were already working (and investing) to implement ES-C2M2 for the enterprise. There are no "least helpful" items.*

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

> *Yes and that guidance is being developed.*

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

> *Yes. Even though we were already working to mature our risk management program and practices, Executive Order 13636 and our engagement in the development of the Framework was an additional catalyst to better engage with the corporate risk management function and make more comprehensive improvements quicker.*

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

> *Yes. Many in the energy sector will continue implement ES-C2M2 to meet the intent of the Framework.*

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?

> *Many in the energy sector will continue implement ES-C2M2 to meet the intent of 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?

> *None.*

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?

> *Yes. In our experience, section 3.5 aligns with our existing policies and approaches.*

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

> *Yes. We continue implement ES-C2M2 to meet the intent of the Framework.*

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?

> *Yes. This was an existing practice that is matured as we continue implement ES-C2M2 to meet the intent of the Framework.*

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

> *Yes. This was an existing practice that is matured as we continue implement ES-C2M2 to meet the intent of the Framework.*

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?

None.

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

Many in the energy sector will continue implement ES-C2M2 to meet the intent of the Framework.