Response to
National Institute of Standards and Technology's Request for Information "Experience with the Framework for Improving Critical Infrastructure Cybersecurity"

October 10, 2014

DISCLAIMER

The views expressed herein are those of select United States Department of Energy employees and are provided solely to inform the NIST framework development process, and should not be interpreted as an official legal or policy position of the Department of Energy.

Department of Energy

Table of Contents

Current Awareness of the Cybersecurity Framework

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?**

Having actively participated in the development of the Cybersecurity Framework, the energy sector stakeholders are generally aware of the Cybersecurity Framework.

Since the release of the Cybersecurity Framework by the National Institute of Standards and Technology (NIST) on February 12, 2014, energy sector stakeholders have collaborated with the Department of Energy (DOE) under the Electricity Subsector Coordinating Council (ESCC) and the Oil & Natural Gas Subsector Coordinating Council (ONG SCC) forums and developed draft *Energy Sector Cybersecurity Framework Implementation Guidance*. The guidance is intended to help energy sector stakeholders:

a. Develop or align existing cybersecurity risk management programs to meet the objectives of the Cybersecurity Framework; and

b. Effectively demonstrate and communicate cybersecurity risk management approach and use of the Framework to both internal and external stakeholders;

The *Energy Sector Cybersecurity Framework Implementation Guidance* will provide further traction towards implementation of the framework in the energy sector.

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?**

Outreach activities by the Department of Homeland Security (DHS), NIST, DOE, and energy sector trade associations are increasing awareness of the Cybersecurity Framework within the sector. These activities include workshops, conferences, web updates, and publications.

In its capacity as the Sector Specific Agency (SSA) for the energy sector as outlined in Executive Order (EO) 13636—Improving Critical Infrastructure Cybersecurity DOE formed a working group with federal and state agencies, regulatory stakeholders, utility owners and operators, and cybersecurity vendors, with the goal of incorporating the use of the Framework with existing efforts to help state and local regulators and state energy policymakers understand and support prudent cybersecurity policies, programs, and investments.

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, the energy sector owners and operators are collaborating with trade associations and public sector partners to receive information and share lessons learned about the Framework.

4. **Is there general awareness that the Framework:**
   a. **Is intended for voluntary use?**
   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?**
   c. **Builds on existing cybersecurity frameworks, standards, and guidelines, and other management practices related to cybersecurity?**

Yes, the current draft of *Energy Sector Cybersecurity Framework Implementation Guidance* which has been developed with industry inputs pivots around the above principles. The sector is cognizant that the Framework is voluntary; and that it can be implemented by building on existing models, standards, and guidelines. The document reflects this understanding by including guidance for a generic approach to framework implementation in the energy sector, followed by an example of how an existing model – the Cybersecurity Capability Maturity Model (C2M2) may be used as a means to implement the Framework according to the generic approach.

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?**

NIST and the SSAs should continue efforts to increase awareness of the Cybersecurity Framework especially among small and medium sized owners and operators of energy sector critical infrastructure. These enterprises may have limited resources requiring tailored outreach and guidance activities

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?**

Relative to the electricity subsector, numerous ONG subsector organizations are multinational organizations. Many of these global organizations are aware and participating in the DOE initiative to develop *Energy Sector Cybersecurity Framework Implementation Guidance*. DOE is not aware of these global organizations' level of awareness or implementation activities beyond their US operations.

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?**

Energy sector regulatory organizations are aware and engaged in Cybersecurity Framework activities. These organizations contributed in the development of the framework and are also engaged in DOE's public-private collaboration effort to develop *Energy Sector Cybersecurity Framework Implementation Guidance*.

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?

The DOE's 'Office of Electricity Delivery and Energy Reliability' (OE) performs numerous outreach activities, e.g., publications, blogs, conferences, and workshops under its various cybersecurity risk management programs such as:

a. Cybersecurity for Energy Delivery Systems (CEDS) program which co-funds research and development projects with industry partners to make advances in cybersecurity capabilities for energy delivery systems.

b. The C2M2 and the Risk Management Process (RMP) Guideline Programs which provide guidance for implementing and evaluating cybersecurity and risk management capabilities.

The DOE has also undertaken a number of outreach and awareness activities with regard to the Framework including dedicating a web page on DOE OE's website describing Framework development and implementation related activities; participation in industry and government hosted panels and conferences to discuss the subject; publication of Federal Register Notices (FRN) to inform sector about DOE's framework guidance activities; and setting up of Cyber.Framework@hq.doe.gov mailbox to streamline public communications on the subject.

The DOE plans to continue Framework outreach and awareness activities in support of EO 13636. These activities will focus primarily on:

a. Strengthening adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities;

b. Providing implementation guidance or supplemental materials to address sector-specific risks and operating environments;

c. Coordinating with owners and operators and relevant stakeholders with regard to section 9 "Identification of Critical Infrastructure at Greatest Risk" of the EO.

d. Leading the Prudent Cybersecurity Investments and Opportunities for Utilities Working Group. The working group will reach out to the state and local regulators and policymakers to increase their awareness of the Cybersecurity Framework and

the current public/private efforts to develop sector-specific guidelines for the Framework's use. This outreach will focus on demonstrating the Framework's usefulness in improving cybersecurity in the critical infrastructure sector and facilitating harmonization among Federal, industry-specific, and state and local cybersecurity practices.

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

NIST should continue its current awareness activities ensuring that all organizations regardless of size gain easy access to relevant information and guidance. Moreover, SSAs should enhance collaboration to support awareness of how cross-sector overlaps are being addressed.

Roadmap for the Future of the Cybersecurity Framework

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?**

   Yes, the "Areas for Development, Alignment, and Collaboration" identified in section 4 of the Roadmap reflect important areas. NIST should continue engagement with private sector to ensure focus on matters relevant to owners and operators.

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?**

   Securing control systems and emerging technologies; sharing cyber threat intelligence; and convergence of physical and cybersecurity are priorities for consideration in future framework activities.

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?**

   The cyber threat and vulnerabilities landscape continues to evolve. As NIST works to advance the usefulness of the Framework, it should be aware of threats, vulnerabilities and challenges posed by developments such as cloud based services, mobile apps, and domestic and international cybersecurity/privacy legislation efforts.