NIST/NARUC Training: NIST Cybersecurity Framework Workshop for Regulators

Date: July 6th
Location: Washington, DC NARUC office, 2nd floor conference room
Participants: 12 attendees (regulators and staff)

9:00 – 10:00 am **Introduction to Workshop** (NARUC)

- Review of what's been happening in cybersecurity around the world
- Explanation of difference between cyber and risk-based structures

10:00 – 11:00 am **Introduction to the NIST CSF** (NIST)

- Explain what the CSF is, why it is important, and what the goals of the Framework are (if done well)
- Discuss CSF structure and what the terms of art in the CSF mean
- How can the CSF be used to align cybersecurity decisions with an organization's objectives
- What do CSF components, attributes, and structures mean in NIST language?
- Audience discussion on what it means to regulators.

11:00 – 11:15 am **Break**

11:15 – 12:45 pm **Application of the CSF** (NIST)

- Explain each of the seven CSF implementation steps
- Show how the CSF applies to the power sector
- Explanation of what you'd expect to see if implementation of the CSF is done well

12:45 – 1:30 pm **Lunch**

1:30 – 2:30 pm **Evaluation of CSF Implementation** (NIST)

- How do regulatory processes in your state enable you to do this type of (audit) work?
- What are some ways to evaluate whether or not implementation at a utility was done well or not? (What are the artifacts, practices and processes, etc. that a regulator could expect to see)

2:30 – 3:15 pm **Examples of Questions Regulators Can Ask Their Utilities** (NARUC)

- Review of various questions that regulators can use to begin dialogues with their utilities to gain an understanding of how they are managing and mitigating their cyber risks, as well as where gaps exist.

3:15 – 3:30 pm **Break**

3:30 – 5:00 pm **Sharing of Participant Experiences** (Audience Members)

- Participants share experiences from home states on using the CSF. Discussion of things that have facilitated learning or hindered it. How well is CSF known, understood, implemented within security operations? How well is CSF known, understood, implemented within regulatory organizations? Is the CSF adding value to the regulatory dialog, or does it have potential to do so? Are there improvements that would make CSF more useful in supporting the regulatory dialog?