Draft

NextGrid: Utility of the Future Study
Reliability, Resiliency, and Cyber Security
Working Group Meeting No. 4
May 22, 2018

Working Group Leaders:
Manimaran Govindarasu
Dominic Saebeler

MEETING SUMMARY

[Note: descriptions of comments and discussion are condensed summaries and paraphrases]

The Working Group Leaders opened the meeting and introduced the presenters.

Agenda Item I: Presentations

Presentations were given by the following:

1.) MISO – Scott Wright
2.) S&C Electric - Jason Lombardo
3.) Illinois Attorney General's Office – Jack Erffmeyer

Please refer to the slide deck presentations for additional information.

Discussion based on presentations:

- Interested in thoughts on the importance of fuel diversity on RTO level.
  - 5 years ago – had 70-75% coal based fuel with the 25-30% nuke and gas. Now more balanced with 45% coal. Also see an expansion in gas and huge buildout in renewables - with a lot more buildout to go. We like to be diverse and have other sources to pull from in case risks or challenges appear for a specific fuel source. Ex.- Wind- have to secure alternative fuel source when wind not blowing.
- Are you noticing regulatory impact for having or not having a diverse portfolio?
  - Because of regulation, we have seen a big push in renewables. We definitely see drive in that area and a lot of projects are already in the que.
- What is the reliability as the impact of renewables increase.

        - There is a degree of durability. Mechanisms must be in place when renewables are not available. Need a system that cover intermittence and the ability to meet any peak times that need to be met.
- NERC CIP – There are many more reliability standards and resources than just NERC CIP. We should be open to looking at other standards than just NERC CIP.
    - Vendors often ask how to be NERC CIP compliant. Its is good to come up with a framework that everyone agrees with and have more realistic metrics and goals that vendors and utilities can meet. Also, providing more guidance on which standards apply to certain aspects of the electric industry (ex. Generation, distribution, transmission etc.)
- Heard in a presentation "citizens should only pay for the resiliency they need." But when factor in natural disasters, the true costs for resiliency come after the fact. How do you quantify the level of investment needed by citizens now?
    - It is possible to arrive to a tolerable level of risk even when facing large consequences for the risk.
- What does supply chain testing look like for an asset with a lifespan of 20-40 years while on the distribution system? How do we take a look at the recovery and valuation of the risk of the asset over the span of the lifetime?
    - This is a tough question to answer and don't know what the answer is right now.
    - This would be a good question to circle back on if possible.
- How and when do you test products?
    - Tests initiate before product gets started. We take a control and run it through blue and red team testing. Then take lessons learned and apply to other products that are under development to make sure those vulnerabilities are resolved before that product is release.

Agenda Item 2: Discussion "Regulation and Compliance"

*Challenge 1 - Achieve a sustainable environment for the **introduction of appropriate standards** and regulations while considering the **operational impact of additional compliance activities**.*

- Opportunities -Effectively navigate introduction of future CIP or other standards considering the number and complexity of existing standards and the large amount of utility staff needed to achieve compliance with existing standards.
- Solutions - Support a regulatory framework that emphasizes actual security over compliance activities.

*Challenge 2 - Achieve **regulatory balance** between utility asset owners and those vendors that design, manufacture, and distribute products to support utility operations. Who has what types of responsibilities? Utilities, vendors, consumers? Currently regulations focus solely on asset owners.*

- Opportunities - Opportunity to offer "NERC CIP Compliant" products. Regional entities currently will work with vendors to ensure meet requirements if properly implemented. Is certifying body needed? Consumers want choice and access, can be incentivized, but need low friction design.
- Solutions - Establish more universal design standards. Create incentives for consumers to take more responsibility for security.

- **Discussion of Questions 1-2:**
    - Reliability measures go beyond just NERC CIP. Recommend having some type of incentives to encourage entities to implement proper cyber security (non financial incentives). Ex. If entity can demonstrate they have or are working on good risk management programs, then perhaps we could extend the audit cycle for a longer duration.
        - We don't want to miss fact that utilities are already doing quite a bit in this area between, NERC, FERC, and internal compliance. It's important to talk about things that are happening rather than giving impression that what we are doing today is not adequate.
        - Agree with both comments. It is very difficult to look into future and design regulatory regimes on things that have not been created yet. The DOW Jones sustainability report dedicated a whole section on cyber security. Would be a good place to look for ideas to design in regulatory framework.
    - We talked about enhanced reliability and resiliency created by EIMA in working groups 1 and 2. There were general consensus on a lot of those principals with the increase in technology and DER on the grid. I think this group is focusing more on the applicability of security in grid operations that EIMA didn't really touch on. Holistically, I think we are looking at this in the right way.
    - Recommend rewording the opportunity section from NERC CIP to a broader term "cyber security products." This will include much more than just NERC CIP.
        - Agree and will revise the wording to include a more generalized practice, products and standards.
    - There are existing labs that do certifications of programs and such. Think is a great conversation to have and something to address.
    - Another challenge is the meaning of common terminology by different stakeholders. Going back to need to define security.
    - compliance – ensure we are also focusing on an open approach where utilities have the ability to share problems and best practices. EX. Airline and automotive industry.
    - We need to define and reword "a certifying body."
    - Always good to reinforce good behavior than punish negative behavior.

Challenge 3 - Navigating the unique Illinois jurisdictional environment when considering: decoupled delivery and supply, MISO/PJM seam, Future Energy Jobs Act (existing nuclear fleet and anticipated increase in solar and wind DER)

- Opportunities - Leveraging standards and best practices from other jurisdictions to support unique aspects of evolving parts of Illinois grid

Challenge 4 - Measuring and assessing the effectiveness of multiple compliance requirements, and a segmented regulatory focus. For example, distribution level regulations are not uniform and not standardized.

- Opportunities - Align compliance activities with various sources, including statutory, policy, and industry standards, as well as federal and state regulations. IOUs with sufficient resources already extend NERC CIP requirements to other assets. Overcoming the possibility that conformity may inadvertently create uniform vulnerabilities.
- Solutions - Resolving or reducing the tension between prescriptive and objectives-based approaches. For example, NIST framework considers compliance a component of risk.

- **Discussion of Questions 3-4**
    - Under leveraging best standards and practices, add from other jurisdictions. Recent orders came down in New Jersey and Maryland to instruct utilities to come up with a working group to come up with a framework to discuss cyber security.
        - Think it was a great process and worked well amongst the stakeholders. There was a frank discussion and a lot of give and take. Feel like will get a good order out of that process.
    - There are national programs that are now focusing on including state players and actors when discussing best practices and problems related to security.
    - Not sure if environment is “unique,” as stated above in the question.
    - Michigan just passed a law exempting cybersecurity discussions from FOIA amongst specified entities.
        - Agree there is a sense to have an open discussion about critical infrastructure without the information getting in the wrong hands.
    - There are probably good engineering reasons why Utilities wouldn’t have distribution level regulations as “uniform and standardized,” as stated above. Would relate back to the Commission’s role in all of this.

Challenge 5 - Achievement of an acceptable level of physical and cyber security across investor-owned, utility co-ops, and municipal-owned utilities.

- Opportunities - Create a flexible regulatory framework that can be customized to appropriately target the necessary level of compliance activities across different entity types.

Challenge 6 - Balancing tradeoffs between meeting regulatory compliance and operational security in the face growing DER integration, EV penetration, and other sources that decrease direct utility control.

- Opportunities - Foster an evolving regulatory approach to supporting and enhancing operational efficiency across the industry. Focusing on effective regulatory environment that achieves utility operational security economically.

- **Discussion of Questions 5-6**
    - From a utility perspective, we do have reliability performance metrics in place through FEJA (outages, customers experiencing reliability outages, etc.) and have met those metrics. We need to be careful on how we state this and not to the assertions that we do not have a reliable Grid to date, but more so is always a work in progress and something we have to stay on top of.
        - Agree – the intent is not to say there is a problem with a particular company, but more of a threshold throughout the whole industry. How do we make sure that everyone is doing the best they can?
        - With a variety of DERS connecting to the grid, it is important to make sure everyone maintains a certain level of security and good for us to recognize at this point.
    - It is to define what is "acceptable," as stated above. Maybe we should rephrase to what is consistent across the different entities.
        - As an individual entity, I would couch it as acceptable value of Risk. This goes beyond much more than just cyber and physical security. It then shows the risk and how to mitigate each risk. Just a broader and better way of looking at the grid.
        - In Illinois, it's the utilities who are responsible for maintain security across the Grid. Utilities valuate risks throughout the entirety of their operations.
        - Depends on how to answer question. If looking at the grid beyond just Illinois, the answer would be different than just considering Illinois and what we already have going.
        - We will go back and work on rewording matrix to include fact that there are metrics that are already in place.
    - A number off people commented on how landscape constantly changes and how regulation should change with it. There is an opportunity to talk about the costs associated with implementing new standards and regulations, and the need for balancing investment for security with cost, and the need for consideration of the cost of adapting to new standards and frameworks.

Challenge 7 - Defining what is an "appropriate level of security" acceptable to all stakeholders. How to define security? What is "secure", who defines "secure enough"?

- Opportunities - If "security" is defined, provides floor. But who defines? When defining security, comprehensively consider reliability and resiliency as well.
- Solutions - Partnerships between and engagement of consumers, utilities, vendors, legislators, regulators, other critical infrastructure asset owners?

Challenge 8 - Reassuring regulators that utilities can and have achieved an appropriate level of preparedness.

- Opportunities - Utilities need to effectively communicate achievement of increase levels of security to satisfy regulator and stakeholder expectations. Increased security should be goal, not increased compliance activity. Emphasize measuring and communicating level of actual security rather than of level of compliance activities.
- Solutions - Create a methodology to assess and measure the impact of compliance requirements to determine whether they actually promote an increase in overall security instead of responsive activities that focus more on achieving compliance but do not result in increased security.

- **Discussion of Questions 7-8**
  - May want take look at the North American Transmission Forum. They have a great amount of information we can pull from.
  - Do we have plans and programs and how often are they exercised, updated, etc. we talk more about response here and how prepared we are.
  - Reiterate increased security is not necessarily the goal. Reducing risk should be our goal and compliance is one aspect of mitigating risk.
  - There are a lot of costs in testing and validating programs already have. We should assure policy makers that risk mitigations are thought about and asserted in the design of systems and such.
    - Have to balance costs of implementing and maintaining security in relation to costs and increased overhead.
    - There is a cost for going back to exercising and checking that systems and plans work. We have to be careful so as to balance the costs associated with those exercises and checks.

Agenda Item 3: General Discussion

- Is there a way to automate security updates rather than having the customer do something to update the security measure?

    - Telecommunications had same issue with internet broadband routers. Over the course of time, we now see more of a network management system where you can push updates during down times and when users are not using products.
- Utilities should have the ability to talk to regulators behind closed doors in relation to security and really tell them what is needed and the ramifications.
- How do security issues come into play when data and information is stored and maintained by a 3rd party or cloud storage?
    - With respect to the cloud, we treat them like a vendor and have some very rigorous cloud requirements. Also have a cloud steering committee as well.
    - Utilities are very conscious of their terms and conditions. (ex. Preventing companies from mining for information, becoming their intellectual property and selling to 3rd parties)

Agenda Item 4: Next Steps

The working group discussed next steps and adjourned the meeting.