NextGrid: Utility of the Future Study
Working Group 3

Meeting No. 5
Cybersecurity
June 14th, 2018

I.) Introduction:

- **The Working Group Leaders opened the meeting:**
  - The matrix is intended to drive conversation around high level and important topics. Would like Feedback that we are tracking in the right areas. Structured to present challenges, opportunities, solutions, action items.
  - Started writing last week, working on first draft. Noticed that matrix didn't work well with all the matrix vacancies. Repeating a lot of content in matrix. Decided to present a one-page view of the key topics – quadrant format. Streamlined wording. When we do have a draft report, will include a chart like this. Went through some of feedback and tweaked matrix topics.
  - Do you think this approach works? Any issues or things to include? Room to expand quadrants a bit – can add a few bullets. Also in process of taking this content and supporting it with a narrative. Will come up with first draft in a week and share with the group.
  - Meeting on 25th – WebEx. Purpose is a drafting working session. Get you something by next Friday to review before the meeting.

II.) Discussion and Questions

- Are you going to have one report with 4 sections and each section has a matrix and overview? Or matrix and overview, then 4 sections?
  - Introduction to our chapter. Flow into each of 4 topics. Each topic has matrix in prose. (Tech chapter, matrix, narrative. People chapter, matrix, narrative).
  - I Like this better for the report.
  - It is about strategy at end of day. I Like this format.
  - Agree, don't want to repeat what is in matrix.
- Agree. As for crossover to other working groups – have we thought about that? Challenge and opportunity to look at business practices and how they relate to technology. Such as the opportunity to adjust the business process from a security point of view.
  - update to group on how we are handling that from broader perspective across all working groups. Internal calls across groups. Created a spreadsheet/matrix crosscutting topical matrix. Put down a series of things we thought impact other groups. We placed "Xs" for overlapping. Each of the working groups will touch on topic in narrative, but a chapter in the larger report that talks about crosscutting issues that impact all the groups. If reading a table of contents, I can see a consistent thread through all of these.
    - For example, business impact of technology and how it ties into security – mentioned in crosscutting section.

- Key action items that can benefit state of Illinois, specifically.
    - Dominic: at this point, our work can apply to any state. Open to more Illinois flavor. Notes and ideas welcome.
- Discuss regulatory policies that exist in IL, or utility or ISO policies that specifically apply in IL. Different than other states/utilities/ISOs.
    - if anyone is impacted by anything, let us know
    - reliability and resiliency. Customer generation. Requirements that there might be -- specific cybersecurity or reliability requirements.
    - Is it an issue in IL?
        - not in a way that is material. From a cybersecurity – universal. Physical is the same.
        - something to keep in mind. Question of whether a good thing or a bad thing? Is uniformity good or bad? Either way. Outlier can protect you, but can stifle economic activity.
    - We can flesh this out and say that this may be an issue in the future.
- Meetings so far: Kickoff, technology, people and process, process went into next meeting then regulation and compliance. Anything we should dig back into?
    - Do you think you have enough material to address the issues? People one – less conversational. Last meeting was great. Any areas we need to take another look at?
    - Challenges in People section, there is redundancy and themes. Less real substantive topics. Reserve the answer to that question until we get through more drafting. Action items needed – just a couple sentences as a way to tie something down to tactical level – action items to recommend to someone in the industry. Individual level or industry level.
    - Even if a viable topic, there is no answer right now, it can be identified as a topic that needs further study.
- Other working groups have had more disagreement/not on same page. Haven't had that with this group. Topic lends itself to agreement. Give people a chance to discuss.
    - what are we missing? Reliability, hospitals are critical. Speed to recover/be resilient. Adapt quickly and respond. Goes beyond electricity. Water even more important. They typically have 48-hour recovery window at hospitals. We haven't talked about the customers and how they are impacted? Do we need to put that in there?
    - Are we in agreement that we are covering the right things? Do we want the customer perspective weaved in?
    - Ameren: Didn't cover how critical interconnected infrastructure is. We are looking at the grid of the future – but without rest of energy sector, can't generate electricity. Can't get things we need without it. We are not just looking at power; we can't generate electricity without other critical sectors as they are Interconnected, especially with increased digitization.
    - Who is our audience? Are we making assumption people know this? Or should we briefly explain? Or is it stating the obvious?
- Would it be beneficial to summarize differences between reliability, resiliency, security, and why it's important and how interconnected they are?
    - Argonne national labs – late 2016. Framework for states to think about resiliency. Interconnectedness, communication, water, electricity.
    - Maybe we can include a reference to that report, with a short write up. Ancillary reading.

    - Resiliency is a crosscutting issue. Presentation for WG 4 – customer and communities. Hospital. Resiliency and recovery critical. Two hospital presentations.
    - Personal information aspects. Driver licenses. You have to have a license to get in the car, but do not need a license to cause havoc on your computer.
    - Like driver license conversation, but lots of concerns. Should have training, but if anyone logged on and they know where you are… Privacy concerns.
- How do we ensure that people are trained and qualified (utility employee, and consumer)? More of proof of education thing – not tracking.
    - Get a Driver's license when 15 years old. No continued education required.
    - Want to make sure people know what they are doing.
    - Another thing to think about – IT background. People who probably have most heartburn and trust the system the least, are the ones most able to cause havoc.
    - Illinois Fusion Center. Some sort of joint center or communication for resiliency and response in case of a regional situation. From a grid reliability standpoint, we are good at that. But maybe not from a cyber standpoint. We have a good crisis management system, and so do the other utilities. But how often do we often exercise jointly for a regional event?
        - One interesting thing happening in other states like NJ, is a well-designed NJ Kick – a center where they specifically take threat info from utilities and process it through as opposed to taking information in and sharing with everyone – trying to help on front end. ISAC and national groups are helping at state level. IL approach is slightly different from other states but evolving to invest in more specific cyber resources? Possibly taking a broader threat approach, instead of cyber. Get a sense that we are trying to move further in that direction and not there yet. To the extent we can collaborate and prevent some things, instead of being reactive it would be positive.
    - Think you are right. Problem we have is willingness of intelligence community to share information in private sector. Pockets of success. Illinois has moved out to create that capability that will allow private sector. Problem is nationwide. If we can't share what we know at classified levels, top secret clearance has nothing to do with information (it's how we obtain that information). Initiative is working with Department of Homeland Security – open up tents. FOIA issues. Illinois is forefront – leading this. In a couple years, that problem will be solved. Have to know what the threat is. Can't share threat because the means to obtain are too valuable, versus the information, how do we get beyond this? Once you blow a source – they shut it down. Lose eyes inside the tents. The solution is to let private sector into the tent with their own problems to explore problems.
    - Is that narrative an appropriate action item? Hoping to have that flushed out over next few years. Will create stronger backdrop to be effective.
    - Yes, have to acknowledge it. Utilities know it is a problem. They want to protect.
    - To reinforce the point, operations standpoint, threat has to be actionable. What we are getting now, week or two late. Need to react in real time.
    - There is a time limits issue. Utilities go to a place and get timely answers.
- Need strategic place to share information, instead of sharing with everyone. How does regulator check with entity? Maybe there's a third place – send it to another place, not to me.

  - Workforce, education – developing inspirational vision – get more excited. Another challenge is convincing people they should want to work in this space. What career aspect looks like. What they can do in the space.
  - Agree. One action item – creating more functional content available to entice a future workforce into this space. I'm observing millennials – visual interactive group coming up. Need more production of videos that show a day in the life who is in the space tackling problems. Interesting things going on – not aware how interesting the field is.
  - A lot of companies have their career page- videos of people on them. I think that when looking for a job, it is too late. Won't look there to begin with. How to take it into schools. Content exists, but merry content and distribute earlier.
  - Emphasize not only exposure to it, but also letting them know it's a viable alternative to working for Apple.
  - Familiarity, talking to people in the space. Coolness of other fields hard to overcome.
  - Agree. There's a misperception you are in security, you're a hacker, know how to fix computers. How can we broaden that? 80% of security groups are not hands-on keyboards. They are understanding business processes… etc. There are other opportunities. Not just one path in security.
  - A lot of the schools are more about cyberbullying and awareness education. Not so much about career.
  - The military does a good job.
  - Whether specific training geared for specific needs. Deficiency in the industry with solar and EE. FEJA was designed to fill a bit of that need with the job training. Industry is trying to find ways to fill specific needs of the deficiency. There are specific trainings, very specific deficiencies in the utility industry. Utility workforce is very old. We are looking to fit the specific needs. Maybe need to look at more than finding ways to train solar installers and EE installers and linemen.
  - Problem I see – look at the kids, middle school, high school. Robotics. Mechanical engineering. We have fewer industry collaborative programs. Needs to become a higher priority initiative. Opportunity for Illinois to create foundation for workforce development. Another point – domestic students. International students find it hard to get a career in cybersecurity. Require experience. Domestic students have a job – scholarship, government.
- Regulation and compliance, technology, process?
  - On technology, one thing we haven't discussed is inverter based tech, to new generation on to system. Smart inverter, IEEE standards might help this a lot, but last Fall in CA, all the inverters of solar caused more of an outage than what might have caused than if inverters stayed online when a momentary fault on system. That issue of inverters on system and their resiliency for functioning during diff voltage and frequency levels – make sure that it doesn't cause a bigger outage.
  - WG 1 technologies. Those should have been identified.
  - How it relates to reliability and resiliency of the grid.
  - Wondering if there is a safety aspect. Solar inverters trip off – backfeed safety issue. Any process improvements that can be made to help with that? So that they can ride through and stay on in these instances?
  - Smart inverter, IEEE standard, just came out April or May. New standard released. It does address a lot of concerns. HI, CA – solar penetration levels, more of an issue. Share

    the article. From safety standpoint, momentary fault – no safety issue. Automatically come back online. Grid stability.
  - Inverter based comments, safety. Huge part of conversation of WG1. Part of inverter based. Communication infrastructure, IT, OT, and whether gap of technology. Ensure reliability, part of the report. Combination of tech and then reliability and resiliency.
  - Clarification. Integrating cloud. Agree with it – caveat that new tech, cloud, AI, Blockchain, will create unknown risks.
- We should have a shorter list of approx. 10 action items. If we have a huge list, readers won't pay attention to it. Should have a shorter list of topics and action items the group finds most important

III.) Adjourn