EPRO SECTOR EXECUTIVE COMMITTEE MEETING, WINTER'17

PLENARY SESSION ONE

RESILIENCE PLANNING AND EMERGENCY COMMUNICATION IN COMPLEX CATASTROPHES

Welcome and Introduction

Andrew Ott, President and CEO, PJM Interconnection

Andy Ott welcomed the participants on behalf of PJM and noted that this was the fourth successive year that PJM had hosted EIS Council. He strongly affirmed the importance of these meeting for PJM and especially their value in helping the company build collaborative, cross-sector relationships. As Ott put it, "We know a lot of people in the power industry, but we don't necessarily know people that we depend on in other industries, and I think this type of forum helps us out."

He singled out for special praise Jonathan Monken, PJM's Senior Director for resilience and strategic coordination, who has been central to PJM's work on building resilience and strengthening its system restoration abilities.

Ott observed that 2017 had been an especially difficult year for all involved in the emergency power and grid resilience. He affirmed that severe hurricane impacts in Houston, Louisiana, Texas, Puerto Rico and the Virgin Islands "give a new sense of purpose to our work here"

Ott recommended viewing "today it as a huge, or at least medium-sized whiteboarding session for resilience Black Sky communication," that is to say, as an opportunity for brainstorming, sharing and disseminating best practices in these areas.

Avi Schnurr, CEO and President, EIS Council

Avi Schnurr began by acknowledging the outstanding group present and saluting their leadership in the Black Sky resilience field. "You are more aware and moving faster in many different sectors on Black Sky issues than any group I think we could find anywhere else," he said.

He affirmed that "the idea of a large-scale power outage which would turn into a long-duration power outage, the cascading failures, the interdependencies creating the dilemma that for any one sector to restore operation, so it would depend on at least minimal operation of its partner sectors; that process is I think pretty well understood, particularly by this group."

Moreover, Schnurr stressed, the impact of Hurricane Maria on Puerto Rico is "the first example of a Black Sky event, with all the cascading failures." As catastrophic as the effects were on the island, "Puerto Rico does have the advantage of having the mainland United States

nearby, available, and heavily engaged to keep that whole process going. That's an advantage that we would not have if it were a very broad issue within the Continental U.S."

Schnurr emphasized that coordination will be absolutely critical to address an event of this scale. There needs to be excellent, and detailed pre-planning between the different sectors if they are to function without the communications technologies that we have become accustomed to.

Coordination, in turn, is comprised of five different aspects, which Schnurr proceeded to detail. "First, is this meeting," he declared, "This is an EPRO Sector Executive Committee," part of a rigorous inter-sectoral process to develop Black Sky Playbooks and integrated planning and collaboration. If we look at the coordination, both processes and the equipment that would be helpful, I think it's fair to say there are five different aspects of the coordination challenge that are particularly key. One way or the other, all five will be touched on to varying degrees today.

Second, there needs to be "a good communications system that will support cross-sector planning when you have an extended power outage, cell phones go down, landlines stop working, and there is a need for all sectors to cross-communicate." Schnurr highlighted the importance of the emergency communication and coordination project that EIS Council is developing with EPRI: the BSX system, and welcomed the presentations on BSX that would be given during the day.

In addition to planning and communication, two other crucial elements of coordination will be situational awareness and decision support. The necessary level of situational awareness requires a simulation model that needs to encompass multiple sectors. Such a model can also provide invaluable decision support, by helping decision makers keep track of resource flows and prioritization choices with machine assistance. EIS Council's Genome project under development is designed to meet both these needs for situational awareness and decision support.

The fifth requirement, that Schnurr described is for "a human coordination process that brings together all of the businesses that represent the vast majority of resources used in the United States. That business coordination across many different corporate sectors obviously has to be matched in parallel by government coordination that has to spin states, federal government, multiple agencies; NGOs need to be tied in." Noting that this process does not exist yet in the United States, Schnurr acknowledged the important work of Dr. Paul Stockton, who, in his excellent fourth volume of the EPRO Handbook series, begins to consider what such a process would look like.

Finally Schnurr reiterated the critical importance of cross-sector communication. In closing he achnowledged and thanked the funders of this work who were present at the meeting: Dr. Pina Templeton, Richard Goodman and Craig Snider.

Keynote Presentation: Black Sky Resilience in the Electric Subsector: Current Status and the Road Ahead

Andrew Ott, President and CEO, PJM Interconnection

Andrew Ott began by noting that we need a sharper definition of resilience, that responds to changes in the power industry and the changing nature of the threats it faces. As Ott put it, "we used to worry about equipment failure and storm-related outages. Those were the two predominant threats. It's different now. Certainly, we still have those. But we're also looking at intentional sabotage, at purposeful attacks on infrastructure and cyber threats as well as threats to the control systems that we depend on."

Ott continued that "although there may be a difference of opinion on what the word resilience means, I don't think there's a difference of opinion on the need for improvement." He stressed that collaboration is essential for building resilience: "no institution can do this alone. Partnership is critical." Ott listed some of PJM's key resilience partnerships, with DOE, DHS, the National Guard as well as with companies in other industries."

As a valuable example of positive collaboration, he cited EIS Council's EARTH EX exercise in August 2017, in which PJM participated. "It's a very well-done exercise," he commented. "It brings a lot more awareness and allows us to learn."

Ott defined PJM's goals in resilience planning as follows: "we're trying to find ways to make sure the systems we operate are more robust, and that they can withstand more, and they can recover quicker." These goals can be broken down into:

1. Planning: physical transmissions planning; planning for emergencies.
2. Operations: How do we operate the grid in a way that's more resilient and adaptable
3. Black start plans and exercises.

Ott then elaborated on three dimensions of resilience that pertain to the power grid.

1. The power grid itself; how to protect critical facilities such as substations that if lost, could cause an outage for an entire region. "Planning the grid in a way that makes critical facilities less critical is important," he noted. Also, PJM is developing ways to operate the grid that allow more flexibility. This will increase the resilience of the grid in the event that part of it is damaged.

2. External networks that are critical to the power grid. These include
   - The gas-pipeline system. In PJM, gas power now accounts for 30% of power generation, up from 5% in 2008. This is a very high level of dependency on gas delivery (although it is lower than that of most other utilities.) The level of dependency raises critical questions. Among those that Ott listed were, "how do we look at fuel security? Do we have liquid-fuel backup? How quickly can that be replenished?"

   - Telecom is another critical external dependency. Ott welcomed the emphasis on communications in several of the rest of the day's sessions.

   - IT networks: The hugely increased level of automation in the power systems helps run the system, but also leaves utilities open to cyber security risks.

- Restoration: Ott noted how, when reviewing PJM's black start plans, it is particularly important to avoid dependencies on a single point of failure, whether it is dependency on a specific fuel or a specific transmission line.

Ott emphasized that it's vital to break down progress towards resilience goals into actionable items. He described how PJM has two kinds of corporate goals: "short-term goals that get done within a year," and "executive strategic goals" that take longer than a year. Executive strategic goals on the restoration side include gaining a deeper understanding of restricted operations, including questions such as "how would we sectionalize the grid operation if we needed to? How would we restore and recover the grid in a more systematic way, and work obviously with our utility partners?"

Another of PJM's long-term resilience projects is the "resilience roadmap" which Ott described as "a way to get from here to here in an actionable sense." One of the major current tasks under this project is to understand gas pipeline contingencies much better: "what happens if we lose a certain section of pipe," (a small such incident occurred recently in Illinois; earthquakes or storms could cause much more serious pipeline failures.)

Ott concluded by mentioning that PJM is also extensively involved in planning for operational resilience, but time did not permit going into details.

Building Resilience: Blue Sky Through Black Sky - Solutions and Critical Issues

Brig. Gen. (Ret.) John Heltzel, Director of Resilience Planning, EIS Council

John Hetzel began by noting the breadth and depth if different people in the room including leadership from all sectors, among them the military, technology leaders and federal government. He hailed the tremendous opportunity for participants to build new relationships and expand theirnetworks.

Hetzel emphasized that Black Sky events are real potentialities. He underscored that if we are not prepared for them, "if we're not thinking about how we recover, and we don't know how we're going to communicate in the case that the landlines get cut, or the cell towers come down, or the radio networks get compromised, or God forbid our nation is attacked, then we put our national security at risk." Hetzel pointed to the aftermath of Hurricane Maria in Puerto Rico as an example of what a very long-term power outage could look like.

Previewing the rest of the day, he announced that this EPRO meeting would have a different format than usual. Instead of a succession of panels, the bulk of the agenda would be comprised of breakout sessions, providing an opportunity for in depth, facilitated discussion of resiliency issues. The sessions would be followed by a short "hotwash" in which representatives of each group would share key issues from their group with the whole meeting.

"Building Resilience:" Morning Breakout Sessions

Track 1 Cyber and Physical Security

Facilitator: Scott Blevins, Communications Sector Coordinator, EIS Council

Track Lead: Tom O'Brien, CIO for PJM

Discussion Resource 1: Brigadier General David Wood, Chief of Joint Staff, Pennsylvania Army National Guard

Discussion Resource 2: Colin Brisson, Manager IT Operations, PJM

Discussion Resource 3: Bryon Koskela, Director, IT Support Service, PJM

Operational Integration of Assets from Public and Private Sector.

Discussion Resource: Brigadier General David Wood, Chief of Joint Staff, Pennsylvania Army National Guard

David Wood discussed the role of the National Guard in protecting both public and private sector assets in an emergency. He explained that if there were to be an attack on the U.S. by an adversary, the active duty military would be facing outward to present the President with response options; the National Guard would be looking inwards to support governors in protecting their states.

He stressed that the primary thing the Guard offers is physical security. The National Guards CST (Civil Support Team) and CPT (Cyber Protection Team) units can offer both protection and assessment.

These CST/CPT teams can support supporting

- State Government IT Infrastructure
- Private Sector infrastructure. (However, in the event of a a major disaster/cyber-attack, the CPT teams would most likely be called in the first instance to support the Federal Government and its agencies.
- General Wood said the PA National Guard has a relationship with First Energy Corp. a major Ohio-based utility.

Discussion Resource 2: Colin Brisson, Manager IT Operations, PJM

Colin Brisson began by noting that PJM is responsible for some 25% of the U.S. Electric grid, including the nation's capital.

He pointed out that threats to the grid are becoming more serious and more diverse with the appearance of hostile state actors who are actively exploring ways to attack US infrastructure. With the increase frequency of threats, PJM is developing ways to automate threat recognition and response, through public- private partnerships and improved intelligence sharing.

Brisson remarked that one of the unresolved issues in a disaster is Unity of Command. "It would be nice to know ahead of time who has the ball," in terms of reacting to threat intelligence, he said.

Discussion Resource 3: Bryon Koskela, Director, IT Support Service, PJM

Bryon Koskela spoke about PJM's approach to cyber-resilience.

He spoke about how this resolves into the following major task - the need to:

- Prevent attacks
- Operate during an attack
- Recover from attack

He talked about how they PJM is set up from the perspective of traditional business continuity planning. Some of the key facilities and capabilities here are:

- Dual data centers in a Hot-Hot configuration
- That they can seamlessly switch between data centers

Koskela stressed that of the most important questions you have to figure out for resiliency is how you ensure redundancy.

He emphasized the unique responsibility of PJM's role as market coordinator between generation, transmission, and distribution facilities. Given this, he said, "the data from our members is our lifeblood. If we don't have our data in order to solve and set price and operate the grid, we're not going to be able to be providing that critical service. That's where we have to work with other industries, specifically telecom, to make sure those connections are good."

He concluded by reiterating the importance of conducting exercises to practice cyber-resilience plans.

Question and Answer Session

Question: The ESCC (Electricity Subsector Coordinating Council) has mutual assistance compact with 130 utilities who have agreed to work together. How could the National Guard be deployed as part of the effort?

General David Wood responded that in the last NDAA (National Defense Authorization Act) congress to establish the Guard's cyber CSTs (Civil Support Team) and CPTs (Cyber Protection Team). They are seeking to run a pilot program in 2018 and have them fully established by 2019. One problem is that US Cyber Command is predominantly outward focused rather than inward focused. In 2018, PJM has committed to deploy the Pennsylvania National Guard as part of their exercise plans.

Question: Colin Brisson had earlier mentioned the **Cyber Risk Information Sharing Program (CRISP)**. A question was presented on how can others use it? What are the next steps?

Colin Brisson responded that the biggest challenge in cyber security is "staying left of the event," that is, spotting warning indicators of an attack early enough to prevent major impacts. He said that CRISP goes back to the intel community to ask for declassification of intelligence so that utilities can respond to it more quickly (- in minutes or hours versus days and weeks). Often, however the information arrives highly classified and utilities will not have any analysts with security clearance for attribution of the sources. The important thing,

Question: Avi Schnurr, CEO and President of EIS Council asked what the speakers thought about what to do about the acute shortages of skilled recovery personnel that would be faced in the event of a cross-sector cyber-attack.

Answers included:

- Putting in place cyber mutual assistance agreements between companies
- Bringing in remote technical support although this would rely on the availability of communications to the remote site
- Accessing the National Guard's CPTs (Cyber Protection Teams.)

Question: How is the National Guard going to allocate their resource during an event in response to the expected demandsbbbbbb?

   a. How the National Guard is prioritized during and actual event is the real challenge. Typically Emergency Management has the lead and the National Guard is prioritized based off of their efforts.
   b. PJM said that they plan on doing more exercises with the National Guard
2. The question came up again that during a Black Sky Event, Who is in-charge?
   a. The comments were; that is the age old question
   b. The comment was during a real event, the answer usually becomes self-evident
3. Dr. Ehud (Udi) Ganani said that cyber in Israel was solved 18 years ago and he broke down elements of Israel's cyber protection program to include:
   a. The CERC (Cyber Event Reporting Center)
   b. Israel's Cyber-Gym, where they have hackers inject events into the system and test everything including hardware.
   c. The National Control Center
   d. The National Cyber Authority and the Israel Electric tabletop exercise
   e. He invited everyone to come to Israel on February 19th to join in the cyber exercise and to see some of these things
4. Matt Wakefield from EPRI (Electric Power Research Institute) took the opportunity to talk about some of their work:
   a. He said they have been working on establishing cyber-security metrics
   b. He said they plan to make all of their work publicly available next week and that it would be all open source
   c. He says they are ready to work with the larger community (cross-sector)
   d. **He said they would like to work with the EIS Council on this**
5. Someone asked, since PJM pulls together resources from generation-transmission-distribution, what keeps the downstream entities in line with cyber-security requirements?
   a. The answer was financial incentives. (NERF?) can inspect them at any time and there are financial penalties for not maintaining systems appropriately.
   b. Generation falls under NERF guidelines
6. One of the participants said he was interested in the CRISP program. His points were:

a. While everyone talks about intel as being sharable, that doesn't mean that it is necessarily shared
b. In his experience a lot of intel flows towards Law Enforcement, the Military, and other government agencies, but a lot of time the information doesn't flow back the other way (including your own information). It isn't bi-directional.
c. He wanted to know if they participated in the CRISP program, would the information be bi-directional and multi-directional