Technology and Security Symposium – Opening address
August 21, 2018
Mark A. Gabriel

Welcome to WAPA's Technology and Security Symposium.

Thank you for joining us today to explore a topic that is keeping the utility industry awake at night: the protection of critical infrastructure. By the end of the day, I expect we will all sleep a little more peacefully knowing that we are taking the necessary steps to ensure the security of our transmission and IT systems.

A key purpose of this symposium is to make the invisible, visible.
In the face of cyber-attacks in both corporate and government offices and physical attacks on infrastructure, WAPA is taking the path of due diligence, investing in and refining our cyber and physical security capabilities.

Risk is traditionally defined as threats times vulnerabilities times impact over cost. You do not have to contemplate that equation for long to fully grasp the importance of risk mitigation. Keeping our system reliable and secure and in compliance with federal and NERC cybersecurity standards is integral to our mission. It also keeps our operational costs down. Strengthening our physical security and cybersecurity mitigates threats, not only to WAPA's operations and performance, but also to you, our customers.

Sharing leading practices and exchanging ideas and lessons learned is central to building a strong, secure and resilient transmission system. Partnership is central to being able to meet and beat the ever-evolving threats to our industry.

As both a federal entity and a Top-10 transmission utility, WAPA must comply with the cybersecurity standards of the federal government and the North American Electric Reliability Corporation. TO name just a few:

- Federal Information Technology Acquisition Reform Act (FITARA)
- Federal Information Security Management Act (FISMA)
- NERC Critical Infrastructure Protection standards
- DOE directives
- Presidential directives

Even without “insider information,” the number and scope of hostile hacking incidents in the news should be a wakeup call for every gas, electric and water utility.

Today, we will be exploring the evolution of WAPA’s security efforts in three different areas.

- Asset management
- Physical security
- Cybersecurity

The progress we have made in refining and standardizing our practices and the steps we are taking to build on that progress.

- $4.3 billion in assets
- 177,000 structures
- 17,360 miles of transmission line
- 316 substations
- 288 transformers
- 659 buildings
- 482 communication sites

WAPA launched the Asset Management Program Improvement Project in 2012, which evolved into our full-time asset management program. Asset Management 2.0, as we call this iteration, provides objective, data-driven justification of capital funding requests and helps to prioritize projects.

Starting with critical transmission equipment, the project standardized the way WAPA collects and processes data on asset condition. Going forward, we will apply this experience to other equipment classes to extend the benefits of asset management across the entire organization.

You will learn more about WAPA's Asset Management program from Chris Lyles during our first panel.

WAPA manages physical risk through a fundamental commitment to security. By dedicating the program to security, integrating regional efforts and emphasizing a culture of compliance, our Office of Security and Emergency Management has made significant strides in the last three years.

- Assessments on all substations completed in FY2017
- A total of 75 second-round assessments in FY2018
- As of Q3, 37 assessments completed [Slide 10]

From 2014 to the present, WAPA has dealt with a total of 80 physical security incidents, which include:

- Break-ins
- Theft
- Sabotage
- Suspicious activity
- Surveillance

We are working with regional stakeholders to implement security countermeasures across the organization, ranging from fence line repairs and signage to security surveillance systems. WAPA recently awarded a Security Integration contract to install video surveillance, access control and intrusion detection systems at several of our most important sites.

Insiders with access, capabilities, knowledge and skills specific to our operations potentially pose just as much risk to our organizations as external threats. OSEM has put several robust personnel security programs in place to help mitigate the potential of an insider threat.
These measures ensure applicants meet all the requirements for federal employment.

Following a 2014 Executive Order, WAPA implemented an Insider Threat Program to help deter, detect and mitigate threat events by government employees that we continue to refine.

In recent audits, OSEM has received consistent high marks from NERC, the Western Electricity Coordinating Council and the Midwest Reliability Organization.

Since 2011, WAPA has been working to create a structured cybersecurity program, equipping it with the right tools to protect our IT infrastructure and staffing it with qualified professionals who understand the urgency of our mission.

The program has implemented measures to ensure that leading practices are standard operating procedure throughout the organization:

- Regular scanning
- Logging of events
- Alerting, patching and updating our system

- Training WAPA employees to detect and guard against threats
- Partnering with DOE and utility industry working groups on cybersecurity pilots and initiatives

The necessity of this investment becomes apparent when you realize that from July of 2017 to May of 2018, the WAPA firewall defended against more than 61 million blocks. In July 2018 alone, there were more than 4 million blocks from sources inside the United States, as well as more than 15,000 from the United Kingdom and 8,000 from China.

WAPA has invested more than 40,000 hours in identifying and mitigating cyber vulnerabilities, implementing network access control to restrict access to differing networks and deploying Secure Enclave Systems Control Centers across our substations.

The Secure Enclave Systems Control Center allows WAPA to securely handle data from operational networks, segregate and analyze it from a cyber perspective, and move the data over to the business network without touching the operational network.

Implementing this data protection solution WAPA-wide has avoided $6.5 million in costs over five years.

Improving compliance processes and procedures is a continuous effort to:

- Improve reliability through lifecycle management
- Comply to federal regulations
- Participate in and respond to regulatory audits
- Anticipate and prepare for increasing cyber threats
- Manage supply chain risk

Our IT team continually evaluates recommendations from CIP audits and mock audits conducted by industry peers, and initiates projects to bring our network into compliance. We see this vigilance pay off when the most recent CIP audit—conducted at our Sierra Nevada region—finds zero violations.

There is satisfaction in seeing our efforts validated by NERC and DOE. But beyond compliance with regulation, protecting our infrastructure assets is simply the best way to do business.

WAPA has factored the need for spending on cybersecurity into our 10-year Technology Capital Investments plan. As critical as this investment is, it is relatively small compared to other capital investments necessary to maintain operational and business excellence.

Although we cannot control all of the pressures driving budget decisions, we strive to turn them into value for our customers. Our investment in physical and cybersecurity translates to mitigating risk to the transmission grid.

All this investments, all these decisions translates for what we bring to you and your customers. Our senior leadership team asks all the time: “What are we spending? How are we spending it? And why are we spending?” I press my staff very hard to make sure that we are extremely clear. We increase costs to make sure the system is reliant and resilient. We make sure that capital investments are being made in the right place.

The Flood Control Act of 1944 says we have to provide hydropower at the “… lowest possible cost consistent with sound business principles.” Most folks hear the “lowest possible cost” part, but they fail to hear the “sound business principles” part.

Figuring out how to mitigate cyber and physical security business IS operating under sound, business principles. It is prudent.

As we also discussed, the regulatory requirements we face are not just about making sure that we dot the Is and cross the Ts, but to make sure that we are strengthening the grid in the process. Some of it is tedious and some of it is expensive, but all of it is required.

To provide the most value, we must also ensure our organization is aligned properly. Several years ago we reorganized our both our IT and physical security programs. We do this to increase efficiencies, control our costs and better serve customers.

In terms of cost containment, many of you know this is near and dear to my heart. Since 2014, we have avoided or saved more than 55 million dollars in costs. That is really important.

Lastly, there are always industry developments. It is an evolve-or-die world. We cannot become Blockbuster or Kodak. We are seeing changes with smart meters and artificial intelligence and blockchain trading. I believe that in the next 3–5 years you're going to see many folks trading out across the regions because it's a financial transaction not an operational transaction. It is a dynamic time in the industry and we need to be thinking years ahead.

In today's environment we all face the same risk and threats to our system. Cyber happens in seconds and there is no such thing as a local event. Talking to each other is our strongest insurance against these events. WAPA has leveraged the resources of the federal government by partnering with the Department of Energy on several programs:

- DOE-wide Integrated Joint Cybersecurity Coordination Center

- Cybersecurity Risk Information Sharing Program – Allows data from participating utilities to be examined by subject matter experts at national laboratories
- Supply chain risk management
- Cooperative protection program

We actively participate in other industry working groups focused on cybersecurity:

- Electricity Information Sharing and Analysis Center
- Multi-State Information Sharing and Analysis Center
- Electric Power Research Institute
- North American Transmission Forum
- DOE Digital Transformation Work Group

You, our customers, must do your part as well by sharing what you learn from your own programs with WAPA and your peers.

Physical security, cybersecurity and asset health form a chain that is only as strong as the weakest link. We are stronger together.