MINUTES OF THE REGULAR MEETING
OF THE
CYBER & PHYSICAL SECURITY COMMITTEE
January 30, 2018

Table of Contents

Subject		Page No.	Exhibit
Introduction		**2**	
1.	Adoption of the January 30, 2018 Proposed Meeting Agenda	3	
2.	Motion to Conduct an Executive Session	4	
3.	Motion to Resume Meeting in Open Session	5	
4.	Cyber Risk Overview	6	4-A
5.	Industry Cyber Security Initiatives and Programs	8	5-A
6.	Security Structure Program Overview	10	6-A
7.	Next Meeting	11	
Closing		**12**	

January 30, 2018

Minutes of the regular meeting of the New York Power Authority's Cyber and Physical Security Committee held at the Authority's offices at 123 Main Street, White Plains, New York at approximately 9:09 a.m.

Members of the Cyber & Physical Security Committee present were:

Michael Balboni - Chairman
John R. Koelmel
Eugene L. Nicandri
Tracy B. McKibben
Dennis G. Trainor

Also in attendance were:

Anthony Picente, Jr.	Trustee
Gil Quiniones	President and Chief Executive Officer
Justin Driscoll	Executive Vice President and General Counsel
Joseph Kessler	Executive Vice President and Chief Operating Officer
Randy Crissman	Senior Reliability and Resilience Specialist - Operations
Kenneth Carnes	Chief Information Security Officer
Karen Delince	Vice President and Corporate Secretary
Thomas Spencer	Senior Director of Enterprise Risk and Corporate Insurance
Lawrence Mallory	Director - Physical Infrastructure Security
Lorna Johnson	Senior Associate Corporate Secretary
Sheila Baughman	Senior Assistant Corporate Secretary

Chairman Balboni presided over the meeting. Corporate Secretary Delince kept the Minutes.

Introduction

Chairman Michael Balboni said this is the first meeting of the Cyber and Physical Security Committee and welcomed committee members, John Koelmel, Eugene Nicandri, Tracy McKibben and Dennis Trainor and the Authority's senior staff to the meeting. He said the meeting had been duly noticed as required by the Open Meetings Law and called the meeting to order pursuant to Section B(4) of the Cyber and Physical Security Committee Charter.

1. Adoption of the January 30, 2018 Proposed Meeting Agenda

Upon motion made by member Eugene Nicandri and seconded by member John Koelmel, the agenda for the meeting was adopted.

2. Motion to Conduct an Executive Session

I move that the Committee conduct an executive session pursuant to the Public Officers Law of the State of New York §105 to discuss matters regarding public safety and security. Upon motion made by member Eugene Nicandri and seconded by member Tracy McKibben, an Executive Session was held.

3. Motion to Resume Meeting in Open Session

I move to resume the meeting in Open Session. Upon motion made by member Eugene Nicandri and seconded by member Tracy McKibben, the meeting resumed in Open Session.

Chairman Balboni said no votes were taken during the Executive Session.

4. Cyber Risk Overview

Mr. Thomas Spencer, Senior Director of Enterprise Risk and Corporate Insurance provided an overview of the Authority's Cyber Risks (Exhibit "4-A"). He discussed some of the efforts that the Risk Management team is undertaking in conjunction with the Information Technology ("IT"), Operational Technology ("OT"), and Physical Security teams to manage the Authority's cyber exposure. Central to those efforts is understanding what the Authority needs to protect.

Physical Assets and Systems - The Authority has to protect its generation and transmission assets and specialized systems such as internal control systems, supervisory control and acquisition systems.

Business Operations - the Authority needs to review its Internet access, business finance and IT systems, as well as its computers and networking devices.

Reputation - the Authority needs to ensure that its reputation to perform as a low-cost, reliable supplier of energy stays intact as it enters the digital age and strive to become the first digital utility.

People - the Authority also needs to protect its employees, retirees, vendors, and suppliers.

Data - the Authority has to protect its employees' personal information, intellectual property, and financial information.

As the Authority transitions into the digital future, it needs to make sure its cyber strategies are flexible enough to meet the challenges of the future, while protecting those assets that it values most.

Risk Management in a Digital World

From a Risk Management point of view, staff considers managing cyber security with a proven framework of four key components:

1) **Identify** risks through easy risk workshops, surveys, customer feedback, and industry forums;
2) **Assess** potential impacts of that risk using that impact's likelihood and velocity scale.
3) **Respond** by prioritizing response strategies based on the Authority's willingness to either accept, transfer, or mitigate those risks; and
4) **Monitor** and correct risk based on data and information received on those risks.

Since conducting the Cyber Risk Workshop, staff has identified cyber risk as an enterprise level risk. Risk Management's staff has continued to work with the cyber IT, OT, and Physical Security teams to improve the Authority's cyber security posture.

Listed below are some of the actions performed by the Risk Management team to make the Authority a stronger organization with regards to Cyber Security.

- **Solidified NYPA's Cyber Security Governance**
  Risk Management has instituted a NYPA Secure Committee, which is a cross-functional team that meets monthly, focusing on cyber and physical security matters, and reports to the Executive Risk Management Committee.

- **Instituted a Business Resiliency Working Program**
  Risk Management works in collaboration with Emergency Management, Disaster Recovery Business Continuity Planning and Physical Security to bolster business resiliency. They meet monthly and discuss NYPA's cyber security, along with other risks that NYPA faces, in order to increase the Authority's business resiliency.

- **Cyber Security Insurance**
  Risk Management purchased Cyber Security Insurance, valued up to $50 million, with a $1 million deductible, as a form of protection against the financial aspects of a cyber event. The insurance covers such incidents as cyber breach, cyber extortion, and cyber events that result in business interruption. There is also a "Reputational" component in the event that the Authority's reputation was damaged due to a cyber event.

- **Resiliency Program**
  Risk Management has developed and established a Reputation Resiliency program where it can identify and prioritize key stakeholders and select an engagement strategy based on NYPA's reputational objectives if a cyber incident were to occur.

- **Cyber Organizational Structure**
  NYPA has enhanced its cyber organizational structure by increasing staff in critical areas, e.g. where greater subject matter expertise is required. In addition, a Chief Information Security Officer has been selected.

In 2018, the Risk Management team will continue to work with Cyber and other groups across the organization with a focus on the areas of risks that have a greater cyber emphasis such as third-party vendor management and insider threat. The team will use the Risk Management framework mentioned previously to identify, assess, respond, and monitor those risks and do a deep dive around those particular areas to ensure that they get an enterprise-level view of the Authority's cyber exposure.

The Risk Management team also plans to engage in business resilience and stress testing in order to look at future scenarios and test the Authority's business model focusing on its cyber aspects, and identifying risks and making corrections, as needed, based on where the team envisions the future of the Authority is going to be from a cyber-perspective. As Risk Management completes these projects and other high-level projects throughout the year, the team will come back to the Committee and update the members on the status and key lessons learned from its Risk Workshops, enterprise-level view of cyber security, insider threat, and third-party vendor management.

5. Industry Cyber Security Initiatives and Programs

Mr. Randy Crissman provided an overview of some of the cyber security initiatives and programs that the industry has undertaken to protect against and mitigate cyber security compromise (Exhibit "5-A").

There are 14 different threats that the electricity sector deems pertinent to the reliable and resilient operation of the electric grid, seven of which have some cyber security element attached to it.

Cyber Security Initiatives and Programs

The Electricity Subsector Coordinating Council ("ESCC") serves as a principle liaison between the electric industry and the federal government in terms of efforts to prepare for, and respond to, national level security events around the country. It is composed of CEOs from about 30 electric utilities, as well as representatives from the federal government, the White House, various cabinet agencies, including Department of Homeland Security ("DHS"), Department of Energy ("DOE"), law enforcement, and national security organizations.

The four areas of focus are as follows:

- Threat information sharing - the information that can be used and action taken from;
- Industry/Government Coordination - for unity of message and unity of effort in the events that occur which affect the Authority;
- Research and Development - what can the Authority do to develop programs and initiatives to help with resilience; and
- Cross-sector Liaisons - how to improve mutual understanding of the dependencies between electricity, telecommunications, finance, and others that are critical during national-level disasters affecting electricity delivery.

Other organizations that are involved in cyber security initiatives and programs include: the Large Public Power Council (comprises the 26 largest public power companies in the country of which NYPA is a member); the American Public Power Association; the National Rural Electric Cooperative; the Edison Electric Institute (the IOUs); the North American Electric Reliability Corporation ("NERC"); the Electric Information Sharing and Analysis Center (a subsidiary of NERC); the North American Transmission Forum; and the Energy Analytic Security Exchange (a collaboration between the electric industry and the financial sector).

Organizations with Cyber Security Initiatives and Programs

1) Electricity Subsector Coordinating Council ("ESCC") - The Strategic Information Coordinating Council ("SICC") was formed among the electricity subsector and the telecommunications and finance sectors to discuss how to improve the coordination of, response to, and recovery from national-level disasters.

After the 2015 NERC GridEx III exercise that tested security preparedness and response across the country, the ESCC established a Cyber Mutual Assistance Program within the electricity subsector. Members of the program may provide or receive resources and support industry response to, or recover from cyber security events that impact reliable electricity delivery. Currently, there are over 130 members in the program, covering about 80 percent of the residential electricity customers in the country.

2) Large Public Power Council ("LPPC") - In 2016, the LPPC established a Cyber Security Task Force of which President Quiniones is a CEO co-sponsor. The task force focuses on collaboration and sharing of cyber security program information. The task force recently published a set of Cyber Security Principles that the LPPC CEOs approved for adoption and which was endorsed by the DOE.

3) American Public Power Association ("APPA") - The APPA has a multi-year contract with DOE, the focus of which is to raise the cyber security posture of its members through various programs. A cyber security insurance program has been established for its members.

4) North American Electric Reliability Corporation ("NERC") - The NERC has established mandatory cyber security standards consisting of ten standards and 28 requirements centered around cyber security.

5) Electricity Information Sharing and Analysis Center ("E-ISAC") - With the support of the LPPC Cyber Security Task Force, the E-ISAC started a new Industry Augmentation Program that involves placing members of electric utility companies in the E-ISAC in Washington, DC for a 3 to 5-day engagement to improve information and knowledge sharing between the industry and the E-ISAC staff that is strengthening the cyber security posture of the grid.

6) North American Transmission Forum ("NATF") - NATF has a program whereby its members can operate with the loss of EMS or SCADA control. This covers almost all of the transmissions in the country.

   The NATF, as well as individual utilities, including NYPA, have devoted resources and efforts to develop, adopt, and test supplemental operating strategies. In the simplest case, these supplemental operating strategies may enable manual operation of assets and systems in the event of a cyber-security compromise that impacts reliable electricity delivery.

6. Security Program Structure Overview

Mr. Kenneth Carnes provided an overview of the Cyber Security Program structure to the members (Exhibit "6-A").

The Authority will continue to focus its security programs and readiness amongst Information Technology, Operational Technology, Physical Security and related teams. Staff will holistically combine integrated response and information sharing as part of iSOC's operations and will continue to leverage the Secure Committee to make sure that they are fast-tracking risks to the Enterprise Risk Management Committee and to the Board, accordingly. In addition, the Authority will continue to train, monitor and assess staff with continuous Awareness and Assessment Phishing tests.

Since the Authority is aware of what it is protecting and who needs access, its programs build security in all of its controls and protections. As the Authority builds-out in 2018, it is partnering with the Energy Power Research Institute and the Large Public Power Council to develop metrics that will insinuate the people, process, and technology status from the tactical level to the high-level financial risk of cyber security. Staff will continue with the activities outlined in the metrics to improve the visibility and reporting on NYPA's security programs.

The Authority will also continue to partner with other organizations in its efforts related to improving information sharing. Cyber Security is very dynamic and it changes daily; therefore, the Authority will need those relationships to support timely and actionable information sharing. In addition, those relationships will give the Authority access to information in order to be ready to respond to a crisis and to be able to leverage its emergency management standardization across Information Technology, Physical security and Emergency Management teams to escalate to the crisis management team of Senior Management; also, how the iSOC is standardizing that information across the board so that it can leverage the intelligence and data even more efficiently and activate the Emergency Operations Center, as needed.

7. Next Meeting

Chairman Balboni said that the next regular meeting of the Cyber and Physical Security Committee is to be determined.

Closing

Upon motion made by member Tracy McKibben and seconded by member John Koelmel, the meeting was adjourned by Chairman Balboni at approximately 10:06 a.m.

Karen Delince

Karen Delince
Corporate Secretary

January 30, 2018

NYPA CYBER & PHYSICAL SECURITY COMMITTEE

EXHIBITS

For

January 30, 2018

Meeting Minutes

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

Cyber Risk Overview

Tom Spencer
Senior Director – Risk Management

January 30, 2018

Risk Management in a Digital World

- Security is IT/OT/Physical and Cyber partnering with Risk Management to actively manage and escalate risk
- The core principles of Risk Management apply as with digitize NYPA
- Leveraging the Cyber Security work in place today to appropriately positions for future Cyber challenges
  - Enhanced 3rd Party Vendor Management
  - Insider Threat Evaluation and Analysis
  - Business Resiliency Stress Testing of alternative future scenarios

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

Industry Cyber Security Initiatives and Programs

Randy Crissman

Senior Consultant – Utility Operations

January 30, 2018

Organizations with Cyber Security Initiatives and Programs

ESCC
Electricity Subsector Coordinating Council

EEI
Edison Electric INSTITUTE

LPPC
LARGE PUBLIC POWER COUNCIL

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

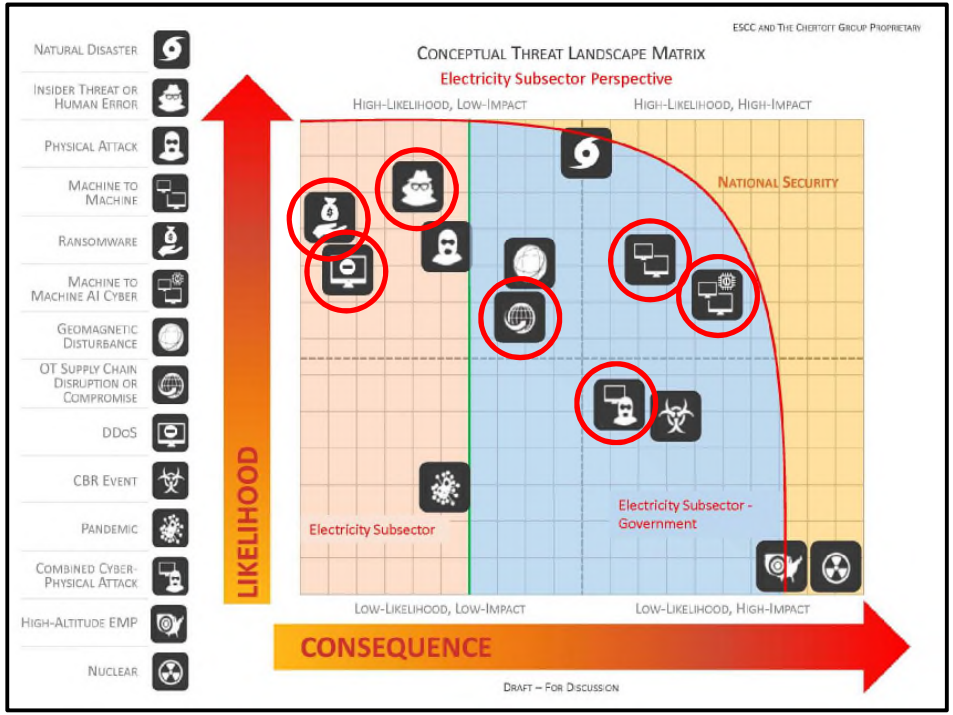
AMERICAN PUBLIC POWER ASSOCIATION

E-ISAC
A DIVISION OF NERC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

North American Transmission FORUM

NRECA
A Touchstone Energy® Cooperative

EASE
Energy Analytic Security Exchange



NEW YORK STATE OF OPPORTUNITY. NY Power Authority | Canal Corporation

Examples of Cyber Security Initiatives and Programs

Electricity Subsector Coordinating Council (ESCC)

- SICC – Electricity Subsector, Telecom, and Finance Coordination
- Cyber Mutual Assistance Program

Large Public Power Council (LPPC)

- Established a Cyber Security Task Force in 2016
- Sharing of Cyber Security Program Practices

American Public Power Association (APPA)

- Multi-Year DOE Grant to Elevate Cyber Security Programs of its Members
- Cyber Security Insurance Program for its Members (via 3rd party)

North American Electric Reliability Corporation (NERC)

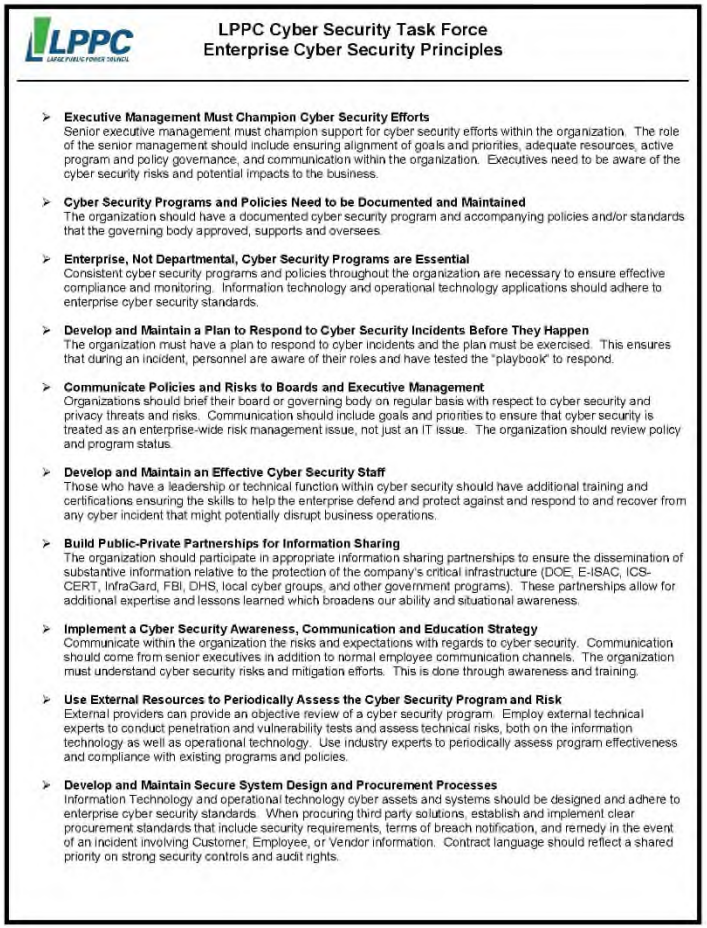
- Mandatory Cyber Security Standards (10 with 28 requirements)

Electricity Information Sharing and Analysis Center (E-ISAC)

- E-ISAC Industry Augmentation Program (pilot with LPPC)

North American Transmission Forum (NATF)

- “Spare Tire” Initiative – Operation With Loss of EMS or SCADA Control



LPPC

LPPC Cyber Security Task Force
Enterprise Cyber Security Principles

- **Executive Management Must Champion Cyber Security Efforts**
  Senior executive management must champion support for cyber security efforts within the organization. The role of the senior management should include ensuring alignment of goals and priorities, adequate resources, active program and policy governance, and communication within the organization. Executives need to be aware of the cyber security risks and potential impacts to the business.
- **Cyber Security Programs and Policies Need to be Documented and Maintained**
  The organization should have a documented cyber security program and accompanying policies and/or standards that the governing body approved, supports and oversees.
- **Enterprise, Not Departmental, Cyber Security Programs are Essential**
  Consistent cyber security programs and policies throughout the organization are necessary to ensure effective compliance and monitoring. Information technology and operational technology applications should adhere to enterprise cyber security standards.
- **Develop and Maintain a Plan to Respond to Cyber Security Incidents Before They Happen**
  The organization must have a plan to respond to cyber incidents and the plan must be exercised. This ensures that during an incident, personnel are aware of their roles and have tested the "playbook" to respond.
- **Communicate Policies and Risks to Boards and Executive Management**
  Organizations should brief their board or governing body on regular basis with respect to cyber security and privacy threats and risks. Communication should include goals and priorities to ensure that cyber security is treated as an enterprise-wide risk management issue, not just an IT issue. The organization should review policy and program status.
- **Develop and Maintain an Effective Cyber Security Staff**
  Those who have a leadership or technical function within cyber security should have additional training and certifications ensuring the skills to help the enterprise defend and protect against and respond to and recover from any cyber incident that might potentially disrupt business operations.
- **Build Public-Private Partnerships for Information Sharing**
  The organization should participate in appropriate information sharing partnerships to ensure the dissemination of substantive information relative to the protection of the company's critical infrastructure (DOE, E-ISAC, ICS-CERT, InfraGard, FBI, DHS, local cyber groups, and other government programs). These partnerships allow for additional expertise and lessons learned which broadens our ability and situational awareness.
- **Implement a Cyber Security Awareness, Communication and Education Strategy**
  Communicate within the organization the risks and expectations with regards to cyber security. Communication should come from senior executives in addition to normal employee communication channels. The organization must understand cyber security risks and mitigation efforts. This is done through awareness and training.
- **Use External Resources to Periodically Assess the Cyber Security Program and Risk**
  External providers can provide an objective review of a cyber security program. Employ external technical experts to conduct penetration and vulnerability tests and assess technical risks, both on the information technology as well as operational technology. Use industry experts to periodically assess program effectiveness and compliance with existing programs and policies.
- **Develop and Maintain Secure System Design and Procurement Processes**
  Information Technology and operational technology cyber assets and systems should be designed and adhere to enterprise cyber security standards. When procuring third party solutions, establish and implement clear procurement standards that include security requirements, terms of breach notification, and remedy in the event of an incident involving Customer, Employee, or Vendor information. Contract language should reflect a shared priority on strong security controls and audit rights.

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Private: Sector Members and Partner Organizations (TLP: Green)
Recommended Audience: E-ISAC Industry Augmentation Program Participants

E-ISAC Industry Augmentation Program

Program Manual
For Pilot with the Large Public Power Council (LPPC)
Rev. 3.2 (Draft)

January 16, 2018

RESILIENCY | RELIABILITY | SECURITY

Products of LPPC Cyber Security Task Force

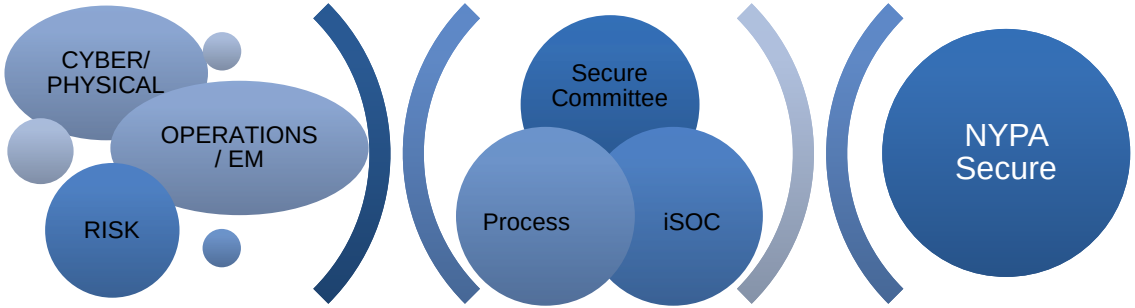
NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

Security Program Overview

Kenneth Carnes
VP & Chief Information Security Officer

January 30, 2018

Security Program Overview



Holistic Focus **Coordinated Response** **Overall Resiliency**

NEW YORK STATE OF OPPORTUNITY. NY Power Authority | Canal Corporation

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

Cyber Risk Overview

Tom Spencer
Senior Director – Risk Management

January 30, 2018

Risk Management in a Digital World

- Security is IT/OT/Physical and Cyber partnering with Risk Management to actively manage and escalate risk
- The core principles of Risk Management apply as with digitize NYPA
- Leveraging the Cyber Security work in place today to appropriately positions for future Cyber challenges
  - Enhanced 3rd Party Vendor Management
  - Insider Threat Evaluation and Analysis
  - Business Resiliency Stress Testing of alternative future scenarios

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

Industry Cyber Security Initiatives and Programs

Randy Crissman

Senior Consultant – Utility Operations

January 30, 2018

Organizations with Cyber Security Initiatives and Programs

ESCC
Electricity Subsector Coordinating Council

EEI
Edison Electric INSTITUTE

LPPC
LARGE PUBLIC POWER COUNCIL

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

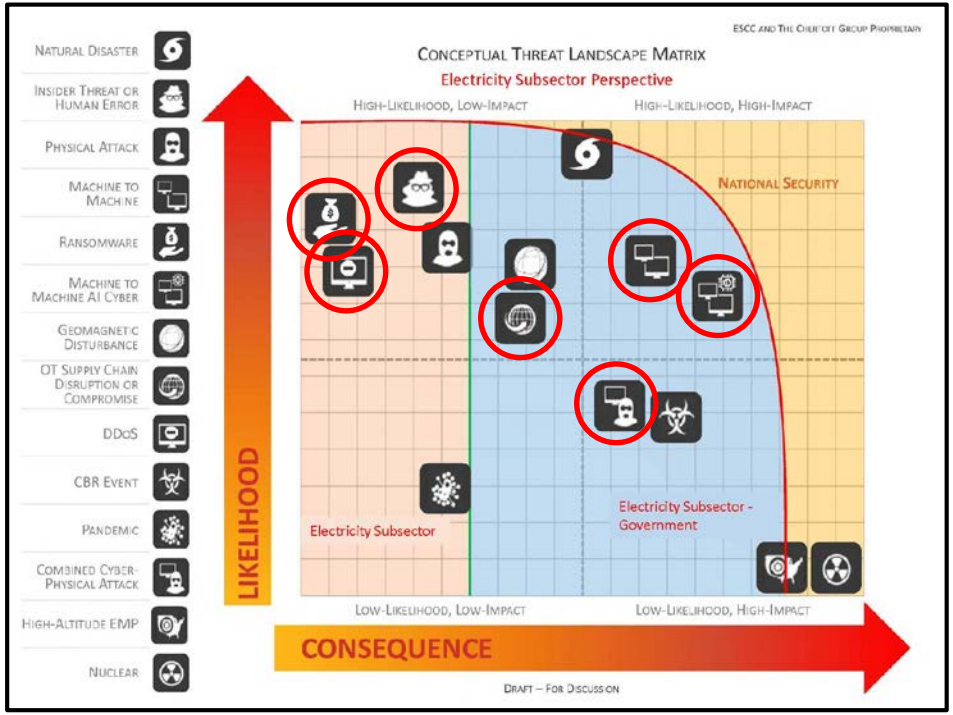
AMERICAN PUBLIC POWER ASSOCIATION

E-ISAC
A DIVISION OF NERC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

North American Transmission FORUM

NRECA
A Touchstone Energy® Cooperative

EASE
Energy Analytic Security Exchange



NEW YORK STATE OF OPPORTUNITY. NY Power Authority | Canal Corporation

Examples of Cyber Security Initiatives and Programs

Electricity Subsector Coordinating Council (ESCC)

- SICC – Electricity Subsector, Telecom, and Finance Coordination
- Cyber Mutual Assistance Program

Large Public Power Council (LPPC)

- Established a Cyber Security Task Force in 2016
- Sharing of Cyber Security Program Practices

American Public Power Association (APPA)

- Multi-Year DOE Grant to Elevate Cyber Security Programs of its Members
- Cyber Security Insurance Program for its Members (via 3rd party)

North American Electric Reliability Corporation (NERC)

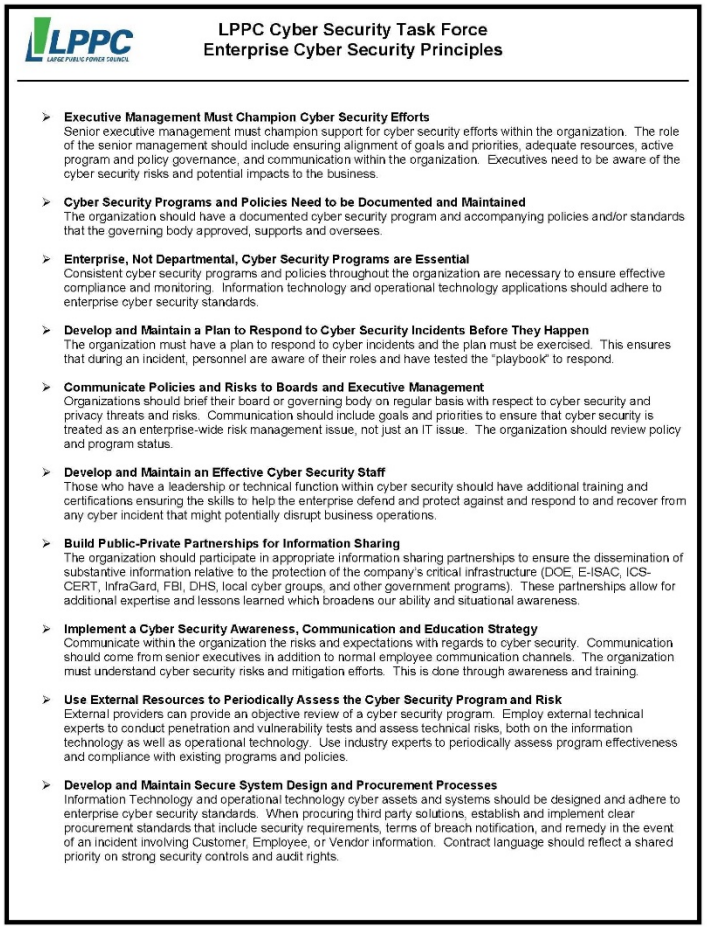
- Mandatory Cyber Security Standards (10 with 28 requirements)

Electricity Information Sharing and Analysis Center (E-ISAC)

- E-ISAC Industry Augmentation Program (pilot with LPPC)

North American Transmission Forum (NATF)

- “Spare Tire” Initiative – Operation With Loss of EMS or SCADA Control



LPPC Cyber Security Task Force
Enterprise Cyber Security Principles

- **Executive Management Must Champion Cyber Security Efforts**
  Senior executive management must champion support for cyber security efforts within the organization. The role of the senior management should include ensuring alignment of goals and priorities, adequate resources, active program and policy governance, and communication within the organization. Executives need to be aware of the cyber security risks and potential impacts to the business.
- **Cyber Security Programs and Policies Need to be Documented and Maintained**
  The organization should have a documented cyber security program and accompanying policies and/or standards that the governing body approved, supports and oversees.
- **Enterprise, Not Departmental, Cyber Security Programs are Essential**
  Consistent cyber security programs and policies throughout the organization are necessary to ensure effective compliance and monitoring. Information technology and operational technology applications should adhere to enterprise cyber security standards.
- **Develop and Maintain a Plan to Respond to Cyber Security Incidents Before They Happen**
  The organization must have a plan to respond to cyber incidents and the plan must be exercised. This ensures that during an incident, personnel are aware of their roles and have tested the "playbook" to respond.
- **Communicate Policies and Risks to Boards and Executive Management**
  Organizations should brief their board or governing body on regular basis with respect to cyber security and privacy threats and risks. Communication should include goals and priorities to ensure that cyber security is treated as an enterprise-wide risk management issue, not just an IT issue. The organization should review policy and program status.
- **Develop and Maintain an Effective Cyber Security Staff**
  Those who have a leadership or technical function within cyber security should have additional training and certifications ensuring the skills to help the enterprise defend and protect against and respond to and recover from any cyber incident that might potentially disrupt business operations.
- **Build Public-Private Partnerships for Information Sharing**
  The organization should participate in appropriate information sharing partnerships to ensure the dissemination of substantive information relative to the protection of the company's critical infrastructure (DOE, E-ISAC, ICS-CERT, InfraGard, FBI, DHS, local cyber groups, and other government programs). These partnerships allow for additional expertise and lessons learned which broadens our ability and situational awareness.
- **Implement a Cyber Security Awareness, Communication and Education Strategy**
  Communicate within the organization the risks and expectations with regards to cyber security. Communication should come from senior executives in addition to normal employee communication channels. The organization must understand cyber security risks and mitigation efforts. This is done through awareness and training.
- **Use External Resources to Periodically Assess the Cyber Security Program and Risk**
  External providers can provide an objective review of a cyber security program. Employ external technical experts to conduct penetration and vulnerability tests and assess technical risks, both on the information technology as well as operational technology. Use industry experts to periodically assess program effectiveness and compliance with existing programs and policies.
- **Develop and Maintain Secure System Design and Procurement Processes**
  Information Technology and operational technology cyber assets and systems should be designed and adhere to enterprise cyber security standards. When procuring third party solutions, establish and implement clear procurement standards that include security requirements, terms of breach notification, and remedy in the event of an incident involving Customer, Employee, or Vendor information. Contract language should reflect a shared priority on strong security controls and audit rights.

E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

E-ISAC Private: Sector Members and Partner Organizations (TLP: Green)
Recommended Audience: E-ISAC Industry Augmentation Program Participants

E-ISAC Industry Augmentation Program

Program Manual
For Pilot with the Large Public Power Council (LPPC)
Rev. 3.2 (Draft)

January 16, 2018

RESILIENCY | RELIABILITY | SECURITY

Products of LPPC Cyber Security Task Force

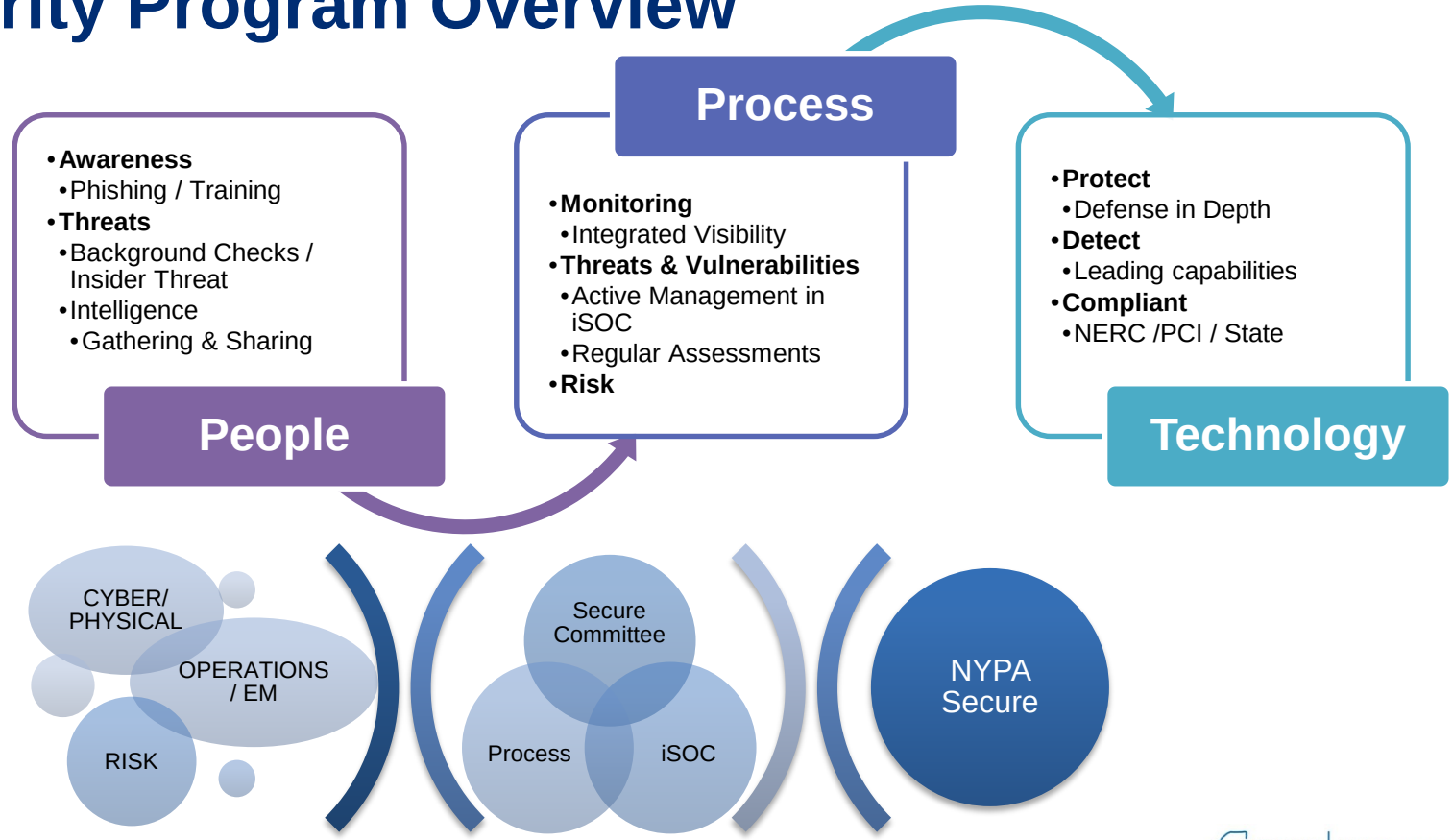
NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation

Security Program Overview

Kenneth Carnes
VP & Chief Information Security Officer

January 30, 2018

Security Program Overview



NEW YORK STATE OF OPPORTUNITY. | NY Power Authority | Canal Corporation