NEW YORK STATE | NY Power Authority | Canal Corporation

MINUTES OF THE JOINT MEETING

OF THE RISK AND RESILIENCY COMMITTEE

July 16, 2024

Table of Contents

July 16, 2024

Minutes of the joint meeting of the New York Power Authority and Canal Corporation's Risk and Resiliency Committee held via videoconference at approximately 10:45 a.m.

Members of the Finance Committee present were:

Cecily Morris - Chair
John Koelmel
Bethaida González
Michael Cusick

Laurie Wheelock - Excused

Also, in attendance were:

Justin E. Driscoll	President and Chief Executive Officer
Adam Barsky	Executive Vice President and Chief Financial Officer
Joseph Kessler	Executive Vice President and Chief Operating Officer
Lori Alesio	Executive Vice President and General Counsel – Legal Affairs
Daniella Piper	Executive Vice President and Chief Innovation Officer
Yves Noel	Senior Vice President and Chief Strategy Officer
Robert Piascik	Senior Vice President and Chief Information & Technology Officer
Alexis Harley	Senior Vice President and Chief Risk and Resiliency Officer
John Canale	Senior Vice President – Strategic Supply Management
Patricia Lombardi	Senior Vice President – Project Delivery
Karina Saslow	Senior Vice President – Human Resources
Charles Imohiosen	Senior Vice President – Communications and External Affairs
Victor Costanza	Vice President and Chief Information Security Officer
Karen Delince	Vice President and Corporate Secretary
James Levine	Assistant General Counsel
Carley Hume	Chief of Staff and Vice President of Policy
Thomas Savin	Senior Director – Enterprise Resilience
Christopher Vitale	Director – Projects
Lorna Johnson	Senior Associate Corporate Secretary
Sheila Quatrocci	Senior Associate Corporate Secretary
Michele Stockwell	Senior Assistant Corporate Secretary

Chair Cecily Morris presided over the meeting. Corporate Secretary Delince kept the Minutes.

Introduction

Chair Cecily Morris welcomed committee members and the Authority's and Canal Corporation's senior staff to the meeting. She said that the meeting has been duly noticed as required by New York State's Open Meetings Law and called the meeting to order pursuant to Section III of the Risk and Resiliency Committee Charter.

1. Adoption of the July 16, 2024 Proposed Meeting Agenda

On motion made by member John Koelmel and seconded by member Michael Cusick, the agenda for the meeting was adopted.

2. DISCUSSION AGENDA:

Chair Cicely Morris invited Ms. Alexis Harley, Senior Vice President and Chief Risk and Resiliency Officer, to provide highlights of staff's report to the members.

Ms. Harley said that two topics of discussion will be presented to the members. The first will be an introductory overview of the emerging risk program highlighting a specific example of an emerging risk that is currently trending around political polarization. The second, a Cyber Security update that will build from takeaways that expert guest speaker, Robert Lee, of Dragos, shared with the Trustees at the May Board meeting.

Chair Morris then invited Mr. Thomas Savin, Senior Director of Enterprise Resilience, to provide highlights of the report to the members.

a. Emerging Risk Overview

Mr. Thomas Savin, Senior Director of Enterprise Resilience, provided an update on emerging risk to the members. He said that in 2021, Emerging Risk was under the "Resilience" umbrella. In 2022, it was formalized, and the Emerging Risk Program was implemented which includes processes for horizon scanning, emerging issues and opportunity analysis, and stakeholder engagement escalating to the Authority's senior leadership and key decision-makers. A third-party was also engaged to support a program maturity assessment.

Emerging Risk Leading Practices

Mr. Savin outlined the core program capabilities the team is seeking to achieve through their maturity efforts. He said that they are based on the ISO 31050 Standard in addition to other leading practices from the vendor. He added that the team also engaged a third-party to support a program maturity assessment.

Core Program capabilities:

- Challenge biases, gathering insights across multiple sources and perspectives, to help separate the noise and drive focus on areas that matter.

- Consider dependencies and interconnections to avoid a fragmented understanding.

- Explore how quickly an uncertainty or trend may manifest to help executives confidently make decisions and communicate with stakeholders.

- Develop an enhanced understanding of ambiguous topics and inform the organization's strategy and monitor changes within the risk profile; and

- Promote innovative thinking and remain agile and dynamic, continuously scanning for changing conditions that can impact the business.

STEEP Framework

The STEEP Framework (Social; Technological; Economic; Environmental; and Political) for identifying trends and uncertainties, as proposed by a third-party, is generally consistent with other emerging risk frameworks. The Authority is evaluating this framework as a method to better track wholly, and report on emerging risk information that is provided to the Board, Senior Management and other decision-makers. This will better enable the team to conduct trending and provide more concise and clear information to the Board members.

Third Party Maturity Assessment – Key Observations and Opportunities

Observations:

- NYPA has strong foundational emerging risk elements and processes, with pockets of excellence, throughout the organization.

- NYPA has a high level of risk awareness, governance, and culture of continuous improvement that the organization can leverage.

Opportunities:

1) Improved collaboration to share emerging risk insights across functions can enhance coordination, minimize surprise.

2) A standard, enterprise-wide process for capturing, monitoring and reporting emerging risk information across the organization can support effective decision-making.

3) Common definitions and assessment methodology can enhance analysis of trends and potential impacts.

4) NYPA's resilience posture can be strengthened by testing assumptions and considering emerging risk scenarios.

The topline objective of these maturity activities is about connecting the right information with the right people at the right time to not only support risk-informed decision-making but also to promote and support longer-term resilience.

Emerging Risk Snapshot – July 2024

The following emerging risks are impactful to the Authority's vision and mission:

1. Artificial Intelligence and Energy Demands

Artificial Intelligence advancements will significantly escalate energy demands and data storage costs. This risk is trending upwards and will become more acute in one to five years and have the potential to cause a moderate business impact.

2. Escalating Political Polarization

Heightened tensions and division among employees and stakeholders holding diverse political perspectives may disrupt operational cohesion and introduce potential new threat vectors into the business lines.

3. Evolving Energy Policies and Regulations

This risk includes technical risks, financial risks associated with the upfront costs of building and upgrading renewable energy infrastructure, political risks related to changes in government policies or public opinion, and operational risks associated with transitioning to renewable energy.

This emerging risk has the potential to impact the Authority's supply chain, and the incentives used within the supply chain that could impact the end cost or result in resources being directed to other industries or initiatives.

4. Increasing Geopolitical Conflict and Uncertainty

The risk of increasing geopolitical conflicts and uncertainty focuses on impacts resulting from potential disruptions to supply chains, heightened cybersecurity threats, new and shifting regulatory and compliance challenges such as procurement prohibitions and increasing financial volatility.

5. Increasing Local Opposition to New Development

This risk was recently added to the Authority's watchlist because there has been increasing levels of coordinated local opposition to new developments which may impede progress toward NYPA's sustainability objectives, hindering the Authority's ability to modernize the grid and meet evolving energy needs of the State and the Authority's customers. This is mostly driven by the complexities and dependencies involved in energizing new generation.

6. Unclear Market Development for Renewables

The risk that unclear or conflicting market signals and conditions could negatively impact NYPA's ability to meet New York's electrification goals and objectives.

Emerging Risk
While staff is proactively monitoring emerging risks, there is no intelligence that indicates a specific threat to the electric sector, New York State, NYPA or Canals.

Escalating Political Polarization
This risk heightens division among employees, stakeholders, or third parties who hold diverse political views and opinions which could manifest and result in a disruption to the Authority's operational cohesion and, by extension, undermine the Authoirty's long long-term objectives. The Authority has engaged the Physical Security, Cyber Security, Ethics & Compliance and Human Resources teams to inform this risk.

This risk could have significant business implications if it were to manifest. The team have seen an increase in this risk since the last monitoring cycle and it is possible that this increase could continue through the November elections. Staff is therefore monitoring this risk through horizon scanning at a greater cadence than other emerging risks on the Authority's watchlist.

Key considerations and Potential Impacts:

Eventful Year Ahead - 2024 is one of the biggest election years in history with 40% of the world's population having an election. Elections shape policy and regulation; policy and regulation impact conflicts, and conflicts can become a crisis.

#Protect2024 – CISA released a centralized repository for security services, training materials, and best practices for addressing cyber, physical, and operational threats stemming from the upcoming US election.

Conflicts Abound – In addition to upcoming elections, perceptions regarding a plethora of seemingly left/right leaning policies and world circumstances may impact behaviors of employees and stakeholders, alone or in aggregate. (e.g., DEI, ESG, Russia/Ukraine war, Israel/Hamas conflict)

Proliferation of Misinformation – Social media platforms provide channels for users to disseminate false information, amplify tensions and embroil organizations unwillingly in political debates, potentially posing reputational harm.

Threat Vectors Expand – As potential conflicts grow, so does the risk of insiders and external antagonistic groups/individuals taking potentially harmful action to demonstrate their viewpoint.

Currently, there are no discrete threats to NYPA, Canals or New York State. NYPA's posture is business-as-usual with heightened awareness and monitoring for early detection mitigation. NYPA also has processes and controls in place to mitigate this emerging risk should it manifest. The Authority continues its active monitoring to ensure that its posture, and any plan mitigations will keep pace with, and are aligned to, this emerging risk as it continues to evolve. Human Resources have identified a new, potential mitigation which can be implemented in advance of elections and will engage with managers to reinforce ethics training and other guidance to maintain a work environment based on mutual respect and neutrality. Also, Physical Security recently created a new dedicated monitoring dashboard for the 2024 elections to support the Authority's heightened monitoring.

b. Cyber Security Update

Mr. Victor Costanza, Vice President and Chief Information Security Officer, provided an update of the report to the members. He said that the team continues to expand its collective defense with the Authority's federal, state, and vendor partners in order to share critical intelligence and keep the Authority ahead of the threat trends. He also elaborated on the team's continued focus on capabilities, recoverability, and testing through functional exercises, reducing user susceptibility through enhanced awareness.

Mr. Costanza then discussed four major points that demonstrate the Authority's ability to identify, detect, protect, respond, and recover regardless of the type of emergent threat to the organization.

2024 Cyber Security Key Focus Areas:

1. IT/OT Cyber Kill Chain Capabilities
   - Optimizing Identity and Access Management to further strengthen 'least privilege' to our environment.
   - Expanding Zero Trust architecture from NYPA to Canals for securing users and applications.
   - Enhancing threat hunting capabilities and sharing with Federal, State, and Industry partners in order to share critical intelligence to keep the Authority ahead of threat trends.

   The team continues to expand its collective defense with federal, state, industry and vendor partners in order to share critical intelligence to keep the Authority ahead of the threat trends. Some recent examples of the achievements include initiatives to building internal network security monitoring within the Authority's operational, technology and digital substation, implementations for greater visibility, and proactive detection of the threats.

   The team worked with New York State partners to expand intelligence sharing capabilities as part of weekly calls with the Joint Security Operations Center participants in order to stay ahead of what may manifest from one area to another and protect the organization before an incident occurs.

   The team further continues to review the cyber hygiene and incident response best practices with the 51 municipal and cooperative customers as part of the collective consortium for cyber which helps to secure the broader NYS electric ecosystem. The team is also working with the Authoirty's customers to ensure that they are secure with the system.

2. Enhancing the ability to Respond
   - Ensuring readiness to respond through execution of functional incident response exercises.
   - Five (5) Regional Exercises successfully completed across NYPA.
   - Simulate realistic scenarios to build muscle memory of incident responders to reduce overall impact.

   The Authority continues to enhance its readiness to respond with tabletop exercises. To date, 5 tabletop exercises have been completed across the various regions to simulate realistic and functional threat scenarios against the Authority's incident response plans. This allows responders to identify, contain, and reduce the overall impact to the Authority's operations and business if an event occurs.

3. Increasing Enterprise Resilience via ability to Recover
   - Maintaining capabilities to restore our systems back to normal business and operation within our tolerance levels.
   - Demonstrating readiness to recover through enhanced Disaster Recovery testing of these capabilities.
   - Incorporation of these recovery scenarios into our incident response drills to ensure reduced time to recover.

   The Authority has the ability to recover its systems back to normal operations within its tolerance levels as defined in its Business Continuity Plans. In the event the Authority is comprised, and system impacted, the Authority will be able to take the appropriate actions to reduce the overall impact to its operations and business. These capabilities are also tested as part of regular drills which are incorporated into the incident response exercises so that the Authority can discuss what it would do if something were to occur, up to, and including going to manual control capabilities, so that the Authority can continue operations seamlessly.

4. Reducing User Susceptibility through Increased Awareness
   - Reinforcing user awareness training to promote safe use of digital resources & ongoing vigilance.
   - Enhancing our user outreach through safety tailgates, security video tutorials, and in-person events.
   - Expanding Cyber Collective Defense Consortium outreach to help our customers protect themselves by increasing security awareness.

   NYPA raises user awareness to address threat trends and increase vigilance and resilience through exercises it conducts with its users, such as phishing exercises and awareness training initiatives to reduce the Authority's user susceptibility to those threats including social media, and disinformation campaigns. This is very critical because the user is the Authority's first line of defense when it comes to being presented with threats. Although the Authority has layered protections, it is up to the user to first identify something that may be presented to them as a threat and avoid it.

Data Trends
Data trends regarding the effectiveness of the program indicate that NYPA's user susceptibility rate have been reduced from 6% to 1%. This is under the 10% industry susceptibility. This was due mainly to the efforts of the Authority's Cyber Awareness Program.

2024 Cyber Key Focus Areas
Threat Trends
Mr. Costanza said that the threat landscape will continue to evolve across the various digital platforms. NYPA Cyber continues to evolve its vulnerability management capability to keep pace with this trend and reduce attacks across those digital ecosystems and maintain zero material cyber security incidents.

NYPA will make investments in cyber security to advance its portfolio capabilities, people, process and technology; remain at the forefront of testing new, innovative cyber security technologies in the face of these threats in order to stay ahead of them; and continue to ensure that security is designed and architected into everything NYPA does, including its expanded authority and all the systems that may be implemented as a part of that initiative; keep the Authority's systems secure; maintain a low-risk appetite and be prepared to quickly recover if a cyber incident were to occur.

3. Next Meeting

Chair Cecily Morris stated that the next regular meeting of the Risk and Resiliency Committee will be held on Tuesday, September 17, 2024.

Closing

On a motion made by member Bethaida González and seconded by member John Koelmel, the meeting was adjourned.

Karen Delince

Karen Delince
Corporate Secretary