PROPOSED AGENDA

NEW YORK POWER AUTHORITY CYBER & PHYSICAL SECURITY
COMMITTEE MEETING

January 25, 2022 at 8:30 a.m.

Videoconference

1. Adoption of the January 25, 2022 Proposed Meeting Agenda

2. Motion to Conduct an Executive Session

3. Motion to Resume Meeting in Open Session

4. DISCUSSION AGENDA:
   a. Cyber Security Update (Eric Meyers and Victor Costanza)
   b. Physical Security Update (Lawrence Mallory)

5. CONSENT AGENDA:
   a. Adoption of the Meeting Minutes of the New York Power Authority Cyber & Physical Security Committee held on July 27, 2021

6. Next Meeting
January 25, 2022

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.
Motion to Resume Meeting in Open Session

Mr. Chairman, I move to resume the meeting in Open Session.
Executive Summary

- Significant improvements delivered during 2021…
  - Launched **security automation** platform to speed detection & response
  - Introduced **behavioral analytics** to help detect never-seen-before attacks
  - Deployed a **protected backup solution** for increased ransomware resilience
  - Introduced a Cyber Collective Defense Consortium to protect the broader NYS ecosystem

- Overcame Increasing Challenges
  - Supply Chain Risks – SolarWinds, Kaseya
  - Increasing ransomware threats
  - Numerous high-profile zero-day vulnerabilities announced – Log4j

- Independent assessments to measure our capability
  - NIST Cyber Security Framework (CSF)
  - Ransomware Readiness Assessment
  - Adversary Attack Simulation
  - Table-top exercises to assess response and recovery capability

- Our 2022 Plan will keep us ahead of the threat landscape
  - Identity & Access Management Program
  - SOC Capability Expansion
  - System hardening and configuration enhancements

---

**2021 By The Numbers:**

- 236K - Threats blocked/day
- 68% - YoY increase in alerts/day
- 96% - Security tools coverage rate
- 10 - Drills and exercises completed
- 5 - Pilot deployments at muni/coops
- 0 - Material cyber security incidents
NIST CSF Assessment

Key Takeaways:
• Comprehensive assessment covering over 100 program elements across 5 domains
• NYPA overall compares favorably to industry peers in the study
• Currently funded program will continue to improve maturity through year-end 2023

Scoring Criteria:
1 - Initial: Ad-hoc processes
2 – Repeatable: Processes defined to where procedures are followed by different people performing the same task
3 – Defined: Processes more rigorously defined and documented using standards, procedures and tools
4 – Managed: Quantitative objectives are for quality and performance are established
5 – Optimized: Processes refined to a level of leading practice. Quantitative continuous improvement in place

Will reassess annually to measure progress and inform future improvements
Identity & Access Management Program
- IDAM Strategy Implementation to support VISION2030
- Privileged Access Management focus

Security Operations Center (SOC) Capability Expansion
- Enhance Internal 24/7 SOC capabilities and process optimization
- Build Cyber Testbed/Range Architecture

Hardening and configuration enhancements
- Firewall Upgrades/Replacements
- System baseline hardening
- Additional network segmentation
- Integration of MDR solution for offline backups

Next Generation Security Architecture
- Security Reference Architecture
- Building in Zero-trust objectives

Continued Foundational Improvements
- Governance Refresh for secure digital enablement
- DLP Capability & Coverage Expansion
- TVM and Cyber Operations Tracking and Metrics enhancements (ITSM integration)
- ICS intrusion detection system implementation with OT
- Partnerships: Cyber Solutions/Pilots for AGILE/Cyber Collective Defense Consortium (CCDC)
Appendices/Backup Slides
The Cyber Kill Chain framework, developed by Lockheed-Martin, is an industry standard method to depict and analyze the process used by a cyber adversary to target victim organizations.

**Objective:** Prevent the adversary from reaching the last stage of the Kill Chain (Act on Objectives)

**How:** Five Ds — Deny, Degrade, Disrupt, Deceive, Destroy adversary capabilities along the Kill Chain

- **Reconnaissance:** Learning about NYPA, its people and systems that they may wish to target. May include passive research on websites and social media as well as active methods (social engineering, etc.)
- **Weaponization:** Creating malware and tools to target NYPA systems that may subsequently be delivered by phishing or “Drive By Downloads” from infected websites
- **Delivery:** Getting the previously deployed malware to a NYPA user, most commonly by e-mail “phishing”
- **Exploitation:** This is where the NYPA user clicks on the link or opens the malicious attachment, an initial piece of malware is installed on the NYPA user’s laptop which then...
- **Installation:** ...automatically reaches out to websites controlled by the adversary to download and install additional pieces of malware/tools which then give the adversary...
- **Command & Control (C2):** ...the ability to remotely access the NYPA user’s PC and begin moving laterally across the NYPA network until they can...
- **Actions on Objectives:** ...complete the objective of their mission which may be to disrupt our operations, steal our data or extort NYPA for ransom (Game Over!)

Kill Chain graphics adapted from Lockheed-Martin
Cyber Kill Chain – How NYPA responds to the bad guys (capabilities schematic)

Kill Chain graphics adapted from Lockheed-Martin

Visible within our network

ON our network!

Preventive
- E-mail filtering
- Multi-Factor Authentication
- Vulnerability Scanning
- Network Security - Firewalls/Web Filtering/Intrusion Prevention

Anti-Virus
- End Point Detection & Response

Detection & Response
- Security Orchestration & Automated Response
- Security Information & Event Mgt
- User Behavior Analytics
- External Network Intrusion Detection
- Internal Network Intrusion Detection
- End Point Forensics
- End Point Detection & Response – IT
- End Point Detection & Response – OT

Intel Partners

Illustrative Examples
(specific product names not shown)
Physical Security Update

Larry Mallory
Sr. Director Security & Crisis Management

January 25, 2022
Regulatory Activity

Module 1: Major Flooding

Crescent-Vischer Ferry Emergency Action Plan Tabletop Exercise 2021

September 22, 2021

Module 3: Misinformation

NERC
North American Electric Reliability Corporation
## Table of Contents

<table>
<thead>
<tr>
<th>Subject</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>1. Adoption of the July 27, 2021 Proposed Meeting Agenda</td>
<td>2</td>
</tr>
<tr>
<td>2. Motion to Conduct an Executive Session</td>
<td>2</td>
</tr>
<tr>
<td>3. Motion to Resume Meeting in Open Session</td>
<td>2</td>
</tr>
<tr>
<td>4. DISCUSSION AGENDA:</td>
<td></td>
</tr>
<tr>
<td>a. Cyber Security Update</td>
<td>3</td>
</tr>
<tr>
<td>b. Physical Security Update</td>
<td>5</td>
</tr>
<tr>
<td>5. CONSENT AGENDA:</td>
<td></td>
</tr>
<tr>
<td>a. Adoption of the Minutes of the Regular Meeting held on January 26, 2021</td>
<td>6</td>
</tr>
<tr>
<td>6. Next Meeting</td>
<td>6</td>
</tr>
<tr>
<td>Closing</td>
<td>7</td>
</tr>
</tbody>
</table>
Minutes of the regular meeting of the New York Power Authority Cyber and Physical Security Committee held at the Clarence D. Rappleyea Building, 123 Main Street White Plains, NY, at approximately 8:30 a.m.

Members of the Cyber & Physical Security Committee present were:

Michael Balboni - Chairman
John R. Koelmel
Eugene L. Nicandri
Tracy B. McKibben
Dennis Trainor
Bethaida González
Anthony Picente, Jr. (excused)

Also in attendance were:

Gil Quiniones  President and Chief Executive Officer
Joseph Kessler  Executive Vice President & Chief Operations Officer
Justin Driscoll  Executive Vice President & General Counsel
Adam Barsky  Executive Vice President & Chief Financial Officer
Kristine Pizzo  Executive Vice President & Chief HR and Administrative Officer
Sarah Salati  Executive Vice President & Chief Commercial Officer
Robert Piascik  Chief Information & Technology Officer
Yves Noel  Senior Vice President – Strategy & Corporate Development
Keith Hayes  Senior Vice President – Clean Energy Solutions
Daniella Piper  Vice President – Digital Transformation / Chief of Staff
Karen Delince  Vice President & Corporate Secretary
Eric Meyers  Vice President & Chief Information Security Officer
Joseph Leary  Vice President – Community & Government Relations
Saul Rojas  Vice President – Enterprise Resilience
John Canale  Vice President – Strategic Supply Management
Lawrence Mallory  Senior Director – Physical Security & Crisis Management
Adrienne Lotto  Senior Director – Energy Security & Resilience Programs
Victor Costanza  Senior Director – Configuration Control and Deputy CISO
Lorna Johnson  Senior Associate Corporate Secretary
Sheila Quatrocci  Associate Corporate Secretary
Andrea Kelli Higgs  Associate Corporate Secretary

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

Committee Chair, Michael Balboni, welcomed the committee members and the Authority’s senior staff to the meeting. He said that 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 July 27, 2021 Proposed Meeting Agenda**

   On motion made by Member John Koelmel and seconded by Member Tracy McKibben, the July 27, 2021 meeting agenda was unanimously adopted.

2. **Motion to Conduct an Executive Session**

   On motion duly made by Member Koelmel, seconded by Member McKibben, and unanimously adopted, an Executive Session was held pursuant to the Public Officers Law of the State of New York §105 to discuss matters regarding public safety and security.

3. **Motion to Resume Meeting in Open Session**

   On motion made by Member Koelmel, seconded by Member McKibben, and unanimously adopted, the meeting resumed in Open Session.

   Chairman Balboni stated no votes were taken during the Executive Session.
4. DISCUSSION AGENDA

a. Cyber Security Update

Mr. Eric Meyers, Vice President and Chief Information Security Officer, presented the Cyber Security Update, which focused on prevention, detection, and response.

Since last reported in January 2021, the Cyber Team completed a reorganization which emphasized capabilities and process optimizations. The Authority’s Cyber Security Program has broadened its focus on three key elements: applying key principles and architecture, leveraging cyber operations, and building a partnership-based ecosystem.

Coordinating with government agencies, industry partners, and the Army Cyber Institute (ACI) at the U.S. Military Academy at West Point, will allow NYPA to share intelligence and leverage best practices across borders. Additionally, applying the tiered “Zero Trust” philosophy of verifying every user, validating every device, and intelligently limiting access, while layering defense with multi-factor authentications, will raise the overall level of cyber resilience.
Cyber Security Program Recap – Prevention, Detection, & Response

• Apply Key Principles & Architecture
  o “Zero Trust” - Verify explicitly, Least Privileges, Assume breach
  o Layered “Defense in Depth” Security Architecture

• Continue to Leverage and build upon our Cyber Ops capabilities in 2021 to monitor, detect, and minimize threats
  o Restructured cyber security in Q1 for improved focus, efficiency
  o New access management strategy

• Leverage and build Partner Ecosystem to share intelligence & coordinate – can’t do it alone

Threat Landscape Update

• Continued stream of widespread, high-profile vulnerabilities/intrusions:
  o Colonial Pipeline ransomware
  o Kaseya supply chain ransomware
  o Microsoft “PrintNightmare”
  o Do not expect the situation to ease up any time soon

• Our Actions:
  o Coordinating with State, Federal, industry partners to learn/share intelligence & best practices
  o Continuous evaluation and upgrade of cyber security portfolio
  o Enhanced resiliency and recovery testing

Even if the profit motive behind ransomware diminishes over time, the risk of destructive cyber events does not as other motives exist
b. **Physical Security Update**

Mr. Larry Mallory, Sr. Director, Security & Crisis Management, presented the Physical Security Report, which highlighted some external partnerships and recent activities.

Since last reported in January 2021, the Physical Security Team has been working with state and federal agencies, and industry partners. One of our partners in the NYS Office of Counterterrorism visited the Zeltmann Power Project in support of their requirement to generate a report on the state of utility security. The Zeltmann Power Project was the last NYPA site visit on the Office of Counterterrorism’s list and the findings will be detailed in a report that will be published in the middle of next year. That program encompasses physical security, cybersecurity, operations, technology, and crisis management. It also provides opportunities to test systems and receive feedback; all in support of the resilience program.

The Physical Security Team received a briefing from the Cybersecurity and Infrastructure Security Agency (CISA) specific to both NYPA and Canals. The federal authority, the Department of Homeland Security, and its partners, reviewed some of the plans, policies, and procedures utilized by NYPA and Canals, and also provided feedback and opportunities for growth. They also collaborated with the Northeast Power Coordinating Council (NPCC), which encompasses part of Canada, and the American Gas Association (AGA). Best practices were shared across sectors and the broad conversation covered design basis, threat process, and NYPA's COVID response.

The Committee requested that staff develop a ransomware tabletop exercise for the members.
5. **CONSENT AGENDA**

On motion made by Member Koelmel and seconded by Member McKibben, the Consent Agenda was adopted.

a. **Adoption of the Minutes of the Regular Meeting held on January 26, 2021**

On motion made and seconded, the Minutes of the New York Power Authority Cyber & Physical Security committee meeting held on January 26, 2021 were unanimously adopted.

6. **Next Meeting**

Chairman Balboni said that the next regular meeting of the Cyber and Physical Security Committee will be held on a date and at a time to be determined.
Closing

On motion made by Member Nicandri and seconded by Member McKibben, by unanimous vote, the meeting was adjourned by Chairman Balboni at approximately 8:58 a.m.

Karen Delince
Karen Delince
Corporate Secretary
Next Meeting

The next regular meeting of the Cyber & Physical Security Committee will be held on Tuesday, July 26, 2022 at a time to be determined.