

## MINUTES OF THE REGULAR MEETING

OF THE

CYBER & PHYSICAL SECURITY COMMITTEE

January 25, 2022

### 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 January 25, 2022 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>2</td>
</tr>
<tr>
<td>a. Cyber Security Update</td>
<td>2</td>
</tr>
<tr>
<td>b. Physical Security Update</td>
<td>8</td>
</tr>
<tr>
<td>5. CONSENT AGENDA:</td>
<td>10</td>
</tr>
<tr>
<td>a. Adoption of the Minutes of the Meeting held on July 27, 2021</td>
<td>10</td>
</tr>
<tr>
<td>6. Next Meeting</td>
<td>10</td>
</tr>
<tr>
<td>Closing</td>
<td>10</td>
</tr>
</tbody>
</table>
Minutes of the regular meeting of the New York Power Authority’s Cyber and Physical Security Committee held via video conference at approximately 8:35 a.m.

Members of the Cyber & Physical Security Committee present were:

Michael Balboni - Chairman  
John R. Koelmel  
Eugene L. Nicandri  
Dennis Trainor  
Bethaida González

Also in attendance were:

Justin Driscoll  Interim President and Chief Executive Officer  
Joseph Kessler  Executive Vice President & Chief Operations Officer  
Lori Alesio  Executive Vice President & Interim 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  
Phil Toia  President NYPA Development  
Yves Noel  Senior Vice President – Strategy & Corporate Development  
Keith Hayes  Senior Vice President – Clean Energy Solutions  
Patricia Lombardi  Senior Vice President – Project Delivery  
Daniella Piper  Vice President – Digital Transformation / Chief of Staff  
John Cabral  Vice President - Digital Services Delivery  
Karen Delince  Vice President & Corporate Secretary  
Eric Meyers  Vice President & Chief Information Security Officer  
John Canale  Vice President – Strategic Supply Management  
Shirley Marine  Vice President – Enterprise Shared Services  
Steven Kalashian  Vice President – Human Resources & Organizational Development  
Lawrence Mallory  Senior Director – Physical Security & Crisis Management  
Adrienne Lotto Walker  Senior Director – Energy Security & Resilience Programs  
Victor Costanza  Senior Director – Configuration Control and Deputy CISO  
Bryan Chan  Director Market Analysis & Hedging  
Christopher Vitale  Financial Performance & Reporting Manager  
Carly Hume  Chief of Staff  
Lorna Johnson  Senior Associate Corporate Secretary  
Sheila Quatrocci  Associate Corporate Secretary

Chairman Balboni presided over the meeting. Corporate Secretary Delince kept the Minutes.
January 25, 2022

**Introduction**

Member John Koelmel said that he will be Acting as Committee Chair until the arrival of Chair Michael Balboni. He 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 January 25, 2022 Proposed Meeting Agenda**

   On motion made by Member Eugene Nicandri and seconded by Member Bethaida González, the January 25, 2022 meeting agenda was unanimously adopted.

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

   On motion duly made by Member Eugene Nicandri, seconded by Member Bethaida González, 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 Eugene Nicandri, seconded by Member Bethaida Gonzalez, 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, and Mr. Victor Constanza, Deputy Chief Information Security Officer, presented an update on the Authority’s Cyber Security Program.

      Mr. Meyers said that in 2021, the cyber program continued to evolve. The Authority faced an unprecedented year in the cyber threat landscape with the widely publicized Solar Winds vulnerability, a seemingly endless list of high-profile ransomware breaches, ending with a high-profile zero-day vulnerability called Log4J, which the team continues to manage.

      As Cyber Security continues to evolve its program, the team took an independent view of its capabilities and maturity to make sure that the Authority was keeping pace with the evolving threat landscape. To that end, the team conducted its first independent assessment of its overall program to measure its capability using the new Cyber Security Framework. They also conducted detailed ransomware readiness assessments and Table-top exercises to assess response and recovery capability.
The NIST CSF Assessment is a midstream assessment of current improvements. It covers over 100 different elements of an overall cyber security program across five key domains. This assessment will continue be repeated annually and will allow Cyber Security to understand how it impacts maturity; measure its maturity against its target state; and inform future investment decisions.

**Cyber Security 2022 Plan**

Mr. Victor Costanza, Deputy Chief Information Security Officer, said that in order to address the evolving threat landscape and enhance the cyber collective defense capabilities and partnerships, Cyber Security has a number of capability improvement projects being implemented in 2022, many of which are already being executed as part of a phased approach, and will be a continuation of the existing Strategic Plan. This includes the Identify and Access Management Program which is a critical foundation for managing user, customer and privileged access management, enhancing the 24-by-7 security event response capabilities, expanded network segmentation of the internal environment for enhanced containment of threats, and threat and vulnerability management tracking integration with the new IT service and asset management platform for greater efficiency and for remediation.

He continued that, as Cyber Security approach the end of its five-year Cyber Security Roadmap this year, the team will further develop and build upon those areas identified in the roadmap to help shape the updated Cyber Resilience Roadmap for 2023, and beyond, with NYPA VISION2030 journey.

Chair Balboni added that Cyber Security is in a period of intense activity as it relates to cyber-attacks. The federal government has recently gotten involved as it relates to zero-trust capability, and Cyber Security is working on providing resources to detect, mitigate and respond to attempts to get into the networks. The Authority has taken on this mission, especially in light of its Digitization Pillar, to make sure that the privileged accesses in the networks are always monitored and secure.
Cyber Security Update

Eric Meyers
VP, Chief Information Security Officer

Victor Costanza
Deputy Chief Information Security Officer

January 25, 2022

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. Inital: 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 set and performance is established
5. Optimized: Processes refined to a level of leading practices: Quantitative continuous improvement in place

Will reassess annually to measure progress and inform future improvements
2022 Plan

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)
Cyber Kill Chain – How the bad guys work

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

How: Five Do's
- Deny
- Deprise
- Disrupt
- Deceive
- Destroy adversary capabilities along the Kill Chain

Reconnaissance
- Learning about NYPA, its people and systems that they may wish to target, may involve human interaction on networks and social media as well as active methods social engineering, etc.

Weaponization
- Creating malware and tools to deliver malware to NYPA systems that may subsequently be delivered by phishing or “Door Prizes” (Physical or Virtual)

Delivery
- Getting the previously deployed malware to a NYPA user, often seeming like a real “phishing”

Exploitation
- This is where the malware exploits the link or opens the vulnerable attachment, an instance of malware is installed on the NYPA work system, which then...

Installation
- Automatically installs client to machines controlled by the adversary in classified and install additional pieces of malware while the user remains oblivious.

Command & Control
- This ability to remotely access the NYPA user’s PC and target it, making it appear as if the NYPA network and they own...

Actions on Objectives
- Completes the objective of the mission which may be to disrupt our operations, steal credentials or extort NYPA for ransom (Dean Devlin)

Cyber Kill Chain – How NYPA responds to the bad guys (capabilities schematic)

Reactive
- End Point Detection & Response
- Malware Analysis & Response
- Network Forensics
- User Behavior Analytics
- Internal Network Intrusion Detection
- Endpoint Forensics
- Host Forensics
- Next Generation Anti-Virus
- Email Filtering
- Multi-Factor Authentication
- Vulnerability Scanning
- Network Security - Firewalls/DH Gateways/Intrusion Detection

Illustrative Examples
(specific product names removed)
b. Physical Security Update

Mr. Larry Mallory, Senior Director of Security & Crisis Management, provided an update on security-related regulatory activities.

NYPA completed the Crescent-Vischer Ferry Emergency Action Plan Tabletop Exercise, 2021, as required by the Federal Energy Regulatory Commission.

NYPA security leveraged the Emergency Action Plan exercise to test its security response, threat escalation and communication plans, enterprise wide. In addition to the typical physical security issues, the team included topics which can influence security, such as misinformation or disinformation campaigns, simulated activities, and threat alert notifications, which led to the implementation of the Authority’s response plans.

In September, NYPA was the subject of a North American Electric Reliability Corporation (“NERC”) Critical Infrastructure Protection Standard Audit. This comprehensive audit covers a number of disciplines. The response to this audit was led by the Authority’s Reliability Standards and Protection team and resulted in zero violations, which speaks to the culture of compliance which NYPA has implemented and fostered.

Through its participation in NERC’s Physical Security Advisory Group, NYPA is also working with NERC in the Electric and Information Training Center to update the Physical Security Design Basis Threat (“DBT”) document and develop an industry training on the application of the DBT. The members will be provided with an update on the progress of the DBT at future meetings.
Physical Security Update
Larry Mallory
Sr. Director Security & Crisis Management

Regulatory Activity

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
5. CONSENT AGENDA

On motion made by Member John R. Koelmel and seconded by Member Bethaida González, the following item on the Consent Agenda was unanimously adopted.

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

6. Next Meeting

Chairman Balboni said that the next regular meeting of the Cyber and Physical Security Committee will be held on Tuesday, July 26, 2022.

Closing

On motion made by Member John R. Koelmel and seconded by Member Bethaida González, by unanimous vote, the meeting was adjourned by Chairman Balboni at approximately 9:47 a.m.

Karen Delince
Karen Delince
Corporate Secretary