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

MINUTES OF THE REGULAR JOINT MEETING
OF THE
CYBER & PHYSICAL SECURITY COMMITTEE
January 26, 2021

Table of Contents

January 26, 2021

Minutes of the regular joint meeting of the New York Power Authority and Canal Corporation's Cyber and Physical Security Committee held via videoconference at 8:00 a.m.

Members of the Cyber & Physical Security Committee present were:

Michael Balboni - Chairman
John R. Koelmel
Eugene L. Nicandri
Tracy B. McKibben
Dennis T. Trainor
Anthony Picente, Jr.

Also in attendance were:

Gil Quiniones	President and Chief Executive Officer
Justin Driscoll	Executive Vice President & General Counsel
Adam Barsky	Executive Vice President & Chief Financial Officer
Joseph Kessler	Executive Vice President & Chief Operations 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
Karen Delince	Vice President and Corporate Secretary
Daniella Piper	Vice President – Digital Transformation / Chief of Staff
John Canale	Vice President – Strategic Supply Management
Eric Meyers	Vice President and Chief Information Security Officer
Joseph Gryzlo	Vice President and Chief Ethics & Compliance Officer
Saul Rojas	Vice President – Enterprise Resilience
Victor Costanza	Senior Director – Configuration Control and Deputy CISO
Lawrence Mallory	Senior Director – Physical Security & Crisis Management
Adrienne Lotto	Senior Director – Energy Security & Resilience Programs
Mary Cahill	Manager – Executive Office
Lorna Johnson	Senior Associate Corporate Secretary
Sheila Quatrocci	Associate Corporate Secretary
Michele Stockwell	Project Coordinator – Executive Office
General Keith Alexander	Chairman & Co-CEO - IronNet Cybersecurity

---

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 January 26, 2021 Proposed Meeting Agenda

On motion made by member Dennis Trainor and seconded by member Tracy McKibben, 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. On motion made by member Dennis Trainor and seconded by member Tracy McKibben, an Executive Session was held.

3. Motion to Resume Meeting in Open Session

Mr. Chairman, I move to resume the meeting in Open Session. On motion made by member Dennis Trainor and seconded by member Tracy McKibben, the meeting resumed in Open Session.

Chairman Balboni said 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, provided an update on the widely reported SolarWinds issue that came to light in early December, NYPA's response, and how NYPA view the situation, going forward (Exhibit "4a-A").

Response to SolarWinds Compromise ("Sunburst")

"Mr. Meyers reported that at the time of the SolarWinds compromise, NYPA was not using one of the vulnerable versions of the SolarWinds software although many companies were using it. In early December, as the situation was developing, there was a lack of clarity on exactly which versions may or may not have been vulnerable; therefore, in an abundance of caution, NYPA took the action to shut down its SolarWinds software and activated its backup monitoring capabilities. Concurrent with that, NYPA immediately began a forensic "hunting" exercise to ensure that the Authority did not have any evidence of the related compromiser in its environment and found none. NYPA is continuing this exercise as part of the Authority's ongoing cyber threat protection and monitoring capabilities.

NYPA also surveyed its supply chain partners to ensure that if any of them had been using SolarWinds or vulnerable versions of it, it would not pose a risk to NYPA. That activity is ongoing, and, to date, no exposures have been found.

In addition, NYPA continues to collaborate with its partners on threat intelligence and other behaviors that could help the Authority understand this situation which is still developing.

State of Cyber Security – Prevention, Detection, & Response

Mr. Meyers then discussed NYPA's approach to mitigating these types of risks as follows:

- Apply Key Principles & Architecture such as "Zero Trust" and Layered "Defense Security Architecture." This will position NYPA, in the future, to be able to contain and minimize the damage if another incident such as this were to occur where the Authority did not have a vulnerable version of the software in its environment and an adversary was able to get in.

- Continue to leverage and build upon Cyber Operations' capabilities to monitor, detect, and minimize threats, looking for unusual network traffic.

- Leverage and build Partner Ecosystem to share intelligence because the Authority only have limited visibility to the overall threat landscape. A key element of the program are the partners that NYPA share intelligence and best practices with; industry organizations, vendors, state, and federal authorities, and the Authority is continuing to expand and grow in that space.

  Most recently, the Authority announced work that it is planning to do with the Army Cyber Institute to increase these threat hunting and detection skills in its own team.

- Another action being taken by the Authority is to survey its technology landscape to understand where the Authority may have potential exposures; where the next SolarWinds is going to come from; where is the next major IT service provider that may be compromised and what impact that might have on organizations like NYPA.

Mr. Meyers ended by saying that he will provide further updates on SolarWinds effects to the Committee. However, it is important to note that NYPA have not observed any adverse impacts related to this incident anywhere within the Authority's ecosystem."

Chair Balboni said this is a growing area of concern, and these types of discussions, in addition to bringing in experts who can help the Authority contextualize the threat, is a very important best practice for NYPA.

5. CONSENT AGENDA

On motion made by member Eugene Nicandri and seconded by member Dennis Trainor the Consent Agenda was adopted.

a. Adoption of the Meeting Minutes of July 28, 2020

On motion made and seconded, the Minutes of the joint NYPA/Canal Corporation Cyber & Physical Security committee meeting held on July 28, 2020 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 time to be determined.

Closing

On motion made by member Dennis Trainor and seconded by member Tracy McKibben, the meeting was adjourned by Chairman Balboni at approximately 9:15 a.m.

Karen Delince

Karen Delince
Corporate Secretary

CYBER & PHYSICAL SECURITY COMMITTEE

EXHIBITS

For

January 26, 2021

Meeting Minutes

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

Cyber Security Update

Robert Piascik – SVP, CIO
Eric Meyers – VP, CISO
Victor Costanza – Deputy CISO

January 26, 2021

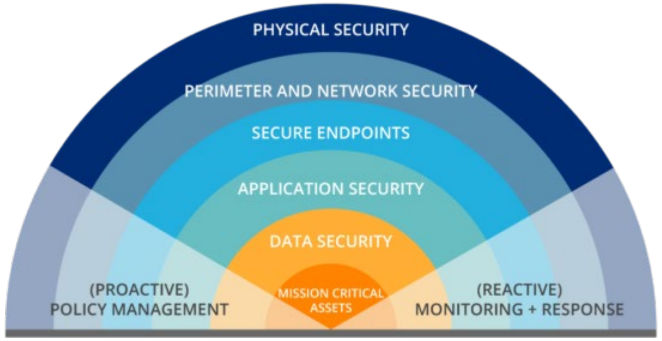
Response to SolarWinds Compromise ("Sunburst")

solarwinds

- Swift Response to identify and mitigate any potential risk
  - Removed SolarWinds software and replaced with alternative
  - Performing "hunting" and forensic monitoring/analysis of entire ecosystem
    - Non- standard files, unusual patterns of access of applications/data, and behavioral analysis
    - Monitoring and action of indicators of comprise and potential malicious activity
  - Surveying NYPA third party entities to determine other potential supply chain impacts
  - Coordinating with State, Federal, industry partners to learn/share intelligence & best practices
  - NYPA participating on Electricity Subsector Coordinating Council "Tiger Team"
    - Coordinate collective response strategies & support Cyber Mutual Assistance activities
    - Develop briefings for industry awareness
    - Coordinate outreach to technology vendors (FireEye, Microsoft, etc.)
- No indication of compromise to date

State of Cyber Security – Prevention, Detection, & Response

- Apply Key Principles & Architecture
  - “Zero Trust” - Verify explicitly, Least Privileges, Assume breach
  - Layered “Defense in Depth” Security Architecture
- Continue to Leverage and build upon our Cyber Ops capabilities in 2021 to monitor, detect, and minimize threats *(Data Loss Protection, Behavior Analytics, Identify/Credential Management, data governance, NERC CIP, etc.)*
- Leverage and build Partner Ecosystem to share intelligence & coordinate – *can’t do it alone*


PHYSICAL SECURITY
PERIMETER AND NETWORK SECURITY
SECURE ENDPOINTS
APPLICATION SECURITY
DATA SECURITY
MISSION CRITICAL ASSETS
(PROACTIVE) POLICY MANAGEMENT
(REACTIVE) MONITORING + RESPONSE

APPA – American Public Power Association
DHS/HSIN – Dept. of Homeland Security/Homeland Security Info. Network
DoE/FERC – Dept. of Energy/Federal Energy Regulatory Commission
EASE – Energy Analytic Security Exchange
E-ISAC – Electricity Info. Sharing & Analysis Ctr
EPRI – Electric Power Research Institute
ESCC – Electricity Subsector Coordinating Council
FBI – Federal Bureau of Investigation
LPPC – Large Public Power Council
MS-ISAC – Multi-State Information Sharing and Analysis Center
NYSIC / DHSES – NYS Intell. Ctr/Div. of Homeland Security & Emergency Svs.
Army Cyber Institute
InfraGard
IronNet/IronDome
Dragos
Deliotte – Cyber Advisory Support
Cisco – *Incident Response Services*