



**MINUTES OF THE REGULAR MEETING
OF THE
CYBER & PHYSICAL SECURITY COMMITTEE
July 26, 2022**

Table of Contents

| <u>Subject</u> | <u>Page No.</u> |
|---|------------------------|
| Introduction | 2 |
| 1. Adoption of the July 26, 2022 Proposed Meeting Agenda | 2 |
| 2. DISCUSSION AGENDA: | 2 |
| a. Cyber Security Mid-Year Update | 2 |
| b. Physical Security Update | 4 |
| 3. CONSENT AGENDA: | 4 |
| a. Adoption of the Minutes of the Meeting held on January 25, 2022 | 4 |
| 4. Next Meeting | 4 |
| Closing | 4 |

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 8:00 a.m.

Members of the Cyber & Physical Security Committee present were:

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

Also in attendance were:

| | |
|----------------------|--|
| Anthony Picente, Jr. | Trustee |
| Bethaida González | Trustee |
| Justin E. Driscoll | Interim President and Chief Executive Officer |
| Philip Toia | President – NYPA Development |
| Lori Alesio | Interim 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 |
| Yves Noel | Senior Vice President & Chief Strategy Officer |
| Robert Piascik | Chief Information & Technology Officer |
| Eric Meyers | Vice President & Chief Information Security Officer |
| Karen Delince | Vice President & Corporate Secretary |
| Saul Rojas | Vice President – Enterprise Resilience |
| John Canale | Vice President – Strategic Supply Management |
| Lawrence Mallory | Senior Director – Physical Security & Crisis Management |
| Victor Costanza | Senior Director – Configuration Control and Deputy CISO |
| Carley Hume | Chief of Staff – Executive Office |
| Lorna Johnson | Senior Associate Corporate Secretary |
| Sheila Quatrocci | Senior Associate Corporate Secretary |
| Michele Stockwell | Project Coordinator – Corporate Secretary |
| Cheyenne Aguayo | Sr. Executive Assistant to President & CEO |

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 26, 2022 Proposed Meeting Agenda

On motion made by Member John Koelmel and seconded by Member Eugene Nicandri, the July 26, 2022 meeting agenda was unanimously adopted.

2. DISCUSSION AGENDA

a. Cyber Security Mid-Year 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 January, the members were provided an update on the independent assessments of cyber security programs that the team performed in 2021, including the NIST Cyber Security Framework (CSF) assessment. In addition, the program of initiatives for 2022 to move the team's maturity forward with respect to that assessment were outlined. The members were also provided an update on the status of those programs as well as a deeper dive on threat and vulnerability management.

Cyber Security programs are on track to deliver measurable improvements.

Identity and Access Management Program

One goal of this program is to bring the next generation approach to Privileged Access Management. This type of access is used by the IT System Administrators to manage the various systems around the NYPA ecosystem which are particularly targeted by cyber adversaries. This new approach was put in place to better manage those accounts as NYPA starts moving towards the cloud in support of its Digitization Program.

Micro Segmentation

Cyber Security is in the process of implementing the first stage of its Zero Trust program termed "Micro Segmentation" which compartmentalizes the IT environment to make it difficult for an adversary to move laterally across the network. To that end, the team has put in place technology that will slow down the ability for an adversary to move around the data center environments without being detected.

Overall, all of the Cyber Security programs are on track or slightly ahead of schedule. The members will be provided additional updates on the programs in the future.

Security Metrics Performance

NYPA continues to evolve its cyber security metrics to provide a better view of the performance of the security program. Two new metrics have been introduced this year; Security Tools Coverage Rate and Vulnerability Management SLA compliance. The metrics have been evolving over time and the team will provide additional metrics that represents the risks faced by NYPA and how effectively the Cyber Security team is managing those risks.

Security Tools Coverage Rate

A wide range of controls have been put in place at end points, various servers, and the network level to achieve herd immunity for the Authority's various devices. A target of 90% was set for this coverage rate; to date, they are exceeding this target.

Vulnerability Management SLA Compliance Rate

NYPA uses a two-tier Service Level Agreement ("SLA") approach for vulnerability remediation which is common in many organizations. Last year, NYPA's standard for remediating its highest criticality vulnerabilities was 48 hours; all the others were remediated within 30 days. On January 1st, the standards were cut in half to 24 hours and 15 days respectively. Against these new SLAs, NYPA has a compliance rate of 96 percent.

Vulnerability Management Performance

NYPA has continued to evolve its vulnerability management capability. Despite an increasing volume of vulnerabilities, NYPA has been able to significantly reduce its remediation cycle-time, as evidenced by the reduced Vulnerability Management SLA standards

NYPA has a comprehensive and robust approach to managing the vulnerability landscape. The Authority continually monitors a wide range of threat and vulnerability sources; thereafter, the Authority executes a response plan to mitigate those risks.

Cyber Collective Defense Consortium

Mr. Victor Costanza, Deputy Chief Information Security Officer, provided a report on NYPA's Cyber Collective Defense Consortium. He said that NYPA is working with the electric municipal and cooperative utility customers as part of its Cyber Collective Defense Consortium ("CCDC") to deploy low or no-cost solutions to help improve their overall security posture. This initiative is aligned with Governor Kathy Hochul's formation of the Joint Security Operation Center ("JSOC"), which is designed to streamline cybersecurity operations and information sharing, as well as protect the Authority's critical infrastructure from cybersecurity threats.

The CCDC solution offerings include the ability to respond and share threat information in a real-time manner through advanced intrusion detection systems. NYPA also has an enhanced ability to identify and correctively remediate vulnerabilities before they can be maliciously compromised by threat actors for these entities through enrollment in the Cybersecurity Infrastructure Security Agency (CISO) cyber hygiene program, as well as the phishing awareness program, to proactively address these threats.

Incident Response Planning

It is important that the Authority's electric municipal and cooperative customers know how to respond in the event of a cyber incident. Therefore, NYPA is assisting these customers in building the processes and skills needed to handle an event should one occur in their technology environment. NYPA provided guidance to eight (8) municipalities in developing an incident response plan and conducted a joint workshop and exercise with a realistic scenario of a threat that impacted their environment and helped them test those plans and identify gaps that needed remediation.

The eight municipalities have shared testimonials with the Authority on the value and benefits that they received, stating that the exercise helped to mitigate their cyber security risks. NYPA plans to expand this workshop to cover all 51 municipalities across the state.

This initiative also helped NYPA Cyber Security team gain insight and intelligence on certain threats that may be impacting smaller utilities that could eventually affect the larger bulk electric system utilities. Therefore, this is a positive initiative, and NYPA looks forward to continuing this incident response workshop and exercise for preparedness and readiness to protect, detect, and respond to cyber events.

b. Physical Security Update

Mr. Larry Mallory, Senior Director of Security & Crisis Management, provided an update on the preparedness and response efforts that are underway in the area of physical security and crisis management. He said that the team has developed a standard for physical security that they execute daily across the enterprise. The plan is fluid, evolves based on current threats and conditions, and is informed by industry partners as well as New York State partner agencies.

Recently, the team leveraged state and local law enforcement and protective Security Advisors from the CISO group of the Department of Homeland Security to observe and participate in a two-part Violent Intruder drill across NYPA. They also reviewed NYPA's response plans, and the team received feedback from them to help improve the Authority's program.

The team is also working on continuing to stress the importance of the "see something, say something" concept of awareness and reporting throughout the organization to the Security staff and employees. They have deployed technology that makes it easier and anonymous to report issues and are providing awareness materials on the indicators of escalation of violence to all employees. Data indicates that 60-percent of people tell at least one person before they engage in a violent act and 40 percent tell at least two people. This means that the eyes and ears of NYPA and Canals employees have become one of the greatest security tools, and the security team is working to leverage that tool and use it to their advantage to help keep everyone safe.

Mr. Mallory ended that he would provide the members further details on Physical Security and Crisis Management's response efforts at future meetings.

3. CONSENT AGENDA

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

a. Adoption of the Minutes of the Regular Meeting held on January 25, 2022

On motion made and seconded, the Minutes of the New York Power Authority Cyber & Physical Security committee meeting held on January 25, 2022 were unanimously adopted.

4. 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 Dennis Trainor and seconded by Member Tracy McKibben, the meeting was adjourned by Chairman Balboni at approximately 8:25 a.m.

Karen Delince
Karen Delince
Corporate Secretary