FOR CONSIDERATION
December 15, 2021

TO: The Oversight and Clean Energy Committee

FROM: Thomas Falcone

SUBJECT: Consideration of Recommendation to Approve the Annual Report on the Former Board Policy on Information and Physical Security

---

Requested Action

The Oversight and Clean Energy Committee (the "Committee") of Board of Trustees (the "Board") of the Long Island Power Authority ("LIPA") is requested to adopt a resolution recommending: (i) approval of the annual report on the former Board Policy on Information and Physical Security (the "Policy") for the period since the last annual review; and (ii) that LIPA has substantially complied with the Policy, which resolution is attached hereto as **Exhibit "A."**

Discussion

By Resolution No. 1500, dated December 18, 2019, the Board adopted the Policy. The Policy delineates the Board's expectations and direction for information and physical security in accordance with public safety, operational, reputational, and compliance requirements and establishes a reporting requirement to the Board on compliance with the key provisions of the Policy. The Policy was last reviewed and amended by the Board at its meeting in December 2020. The Policy was supplanted by a new Information Technology and Cybersecurity Policy at the Board's November 17, 2021 meeting; however, Staff is reporting on compliance with the prior Policy for activities through November 2021.

Compliance with the Policy

LIPA Staff recommends that, for the reasons set forth below, the Board find that LIPA has - substantially complied with the Policy. Compliance with each element of the Policy is discussed in detail below.

The Policy provides that "LIPA and its Service Provider will undertake, at a minimum, the following activities each year":

"Annual reviews of the overall maturity of the cyber and physical security programs of LIPA and its Service Provider, consistent with industry best practices"

- LIPA and its service provider, PSEG Long Island, have adopted the NIST Cybersecurity Framework (CSF) to drive improvements to their cybersecurity programs. The Framework focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the risk management processes, including guidance on People, Process, and Technology to implement defense in depth for the enterprise.

- LIPA and its service provider, PSEG Long Island, have adopted NERC's Physical Security Standard (CIP-2 and CIP-14) to protect LIPA's T&D assets. The physical security of each of the T&D assets is derived from a risk assessment of each asset and its impact on the power grid.

"The Service Provider will conduct quarterly internal and annual third-party vulnerability assessment and penetration testing of all Information Technology (IT) and Operational Technology (OT) assets and vulnerability assessment of facilities and functions every three years. The Service Provider will confidentially submit the vulnerability assessment and penetration testing reports, management action plans, and monthly progress report on remediation to LIPA' s Chief Information Officer"

- PSEG Long Island Cybersecurity: PSEG engaged a third-party consultant to perform a vulnerability assessment and penetration test late in 2020. Due to COVID-19 limitations, the assessment was concluded in the first quarter of 2021. PSEG Long Island reported the remediation of all critical, high, and medium risks identified as a result of the assessment. Management Action Plans were not submitted to LIPA. However, PSEG Long Island reports monthly on progress to close the findings. PSEG Long Island also has a program of monthly vulnerability scanning of all assets, which are tracked in a comprehensive database and are addressed throughout the year. The Request for Proposal for the 2022 assessment has been released, and responses are pending.

- LIPA Cybersecurity: LIPA engaged a third-party firm to conduct a vulnerability assessment and penetration test and performed focused timeboxed attack and penetration testing of hosts on LIPA's corporate network, including servers, workstations, and other network devices available through the internal environment. Remediation plans were developed and are being implemented. Significant improvements in the LIPA's cybersecurity management practices were made in 2021.

- PSEG Long Island Physical Security: FERC reliability standards require transmission owners or operators to perform a risk assessment of their systems to identify "critical facilities," evaluate the potential threats and vulnerabilities to those identified facilities and develop and implement a security plan designed to protect against physical attacks on those identified critical facilities. PSEG Long Island conducts Security Vulnerability Inspections (SVI) at 53 critical and NERC facilities and Physical Security Inspections (PSI) at all LIPA sites. A computer database is used for tracking inspections and the management of NERC CIP Physical Security requirements. In addition, a "Red Team" penetration test is conducted to assess the Security Command Center response.

- In 2021, PSEG Long Island performed annual SVIs for 51 of the 53 identified critical facilities, with the final two facilities scheduled for completion in December 2021. There were no critical physical security deficiencies discovered during these inspections.

"The Service Provider will conduct an independent annual NIST Cybersecurity Framework and COBIT 2019 Maturity Level assessment by an assessor approved by LIPA and confidentially

submit assessment reports and management action plans, including planned initiatives to achieve targeted COBIT Maturity Level 4 (Quantitatively Managed) along with NIST CSF Tier 3 (Repeatable) by September 2021 and COBIT Maturity Level 5 (Optimizing) along with NIST CSF Tier 4 (Adaptable) by September 2022"

- PSEG Long Island will not meet its NIST - CSF/COBIT Maturity target for 2021 established in the Board policy. PSEG Long Island conducted the NIST Cybersecurity Maturity Level assessment and developed the work plan to improve the maturity level. PSEG Long Island report on progress at monthly oversight meetings. However, the evaluation and the work plan have not been submitted to LIPA. PSEG Long Island did not complete the COBIT maturity assessment. The NIST-CSF maturity target has been incorporated into the reformed contract default metrics.

"The Service Provider will develop initial 3-Year Cyber and Physical Security Strategic Plans and submit them to LIPA by June 2021; the Service Provider will review and/or update the respective Strategic Plans at least annually to consider the changing threat landscape and/or mitigation opportunities"

- To date, PSEG Long Island has not submitted an initial 3-Year Cybersecurity Strategic plan.

- In June 2021, PSEG Long Island delivered to LIPA a report outlining their physical security plans and priorities. LIPA reviewed the plan and believes there is room for improvement. In 2022, LIPA will be engaging an outside consultant to review PSEG Long Island's physical security plans and practices and make recommendations for enhancements to be included in the 2023 budget.

"The Service Provider will develop and submit to LIPA an annual work-plan in Q4 of each year for the subsequent year, guided by the Cyber and Physical Security Strategic Plans"

- PSEG Long Island has not developed nor submitted the annual Cybersecurity Work Plan for 2022.

- Though formal Strategic and Work Plans have not been developed for Physical Security, PSEG Long Island has provided a Project Justification Document (PJD) describing 2022 planned work, which entails security upgrades at two substations. Going forward, LIPA will endeavor to align the Board Policy with the Budget and PJD processes.

"The Service Provider shall comply with all applicable standards, directives, and guidance issued by regulatory or industry advisory bodies, including the North American Electric Reliability Corporation, Federal Energy Regulatory Commission, Department of Energy, Department of Homeland Security, and New York State Department of Public Service; This would include Annual self-assessment for compliance with NERC. Quarterly reporting of any incidents of non-compliance with the applicable standards"

- In 2021 Northeast Power Coordinating Council (NPPC) Inc. conducted a scheduled audit of PSEG Long Island's NERC compliance. The audit period was from September 28, 2018, to October 30, 2020, for CIP; February 28, 2015, to October 30, 2020 (DP: Distribution Provider, TO: Transmission Owner) and November 30, 2017, to October 30, 2020 (TOP: Transmission Operations, TP: Transmission Planner) for O&P (Operations and Planning); and covered the DP, TOP, TO and TP function(s). The audit process included a review of evidence submitted to demonstrate compliance and SME interviews conducted virtually. The audit scope included 15 standards and 46 requirements. The audit findings resulted in three potential non-compliance findings, for which remediation has been addressed. None of these findings were related to physical security.

"The Service Provider will confidentially report no less than quarterly to LIPA's Chief Information Officer: Service Provider's compliance with industry and regulatory standards and exceptions. The effectiveness of the Security Programs and Policies, as indicated by various security-related Key Performance Indicators (KPIs). Implementation of additional defensive technology initiatives. Security incidents, responses, and their impact."

- In compliance with this policy requirement, PSEG Long Island staff provided monthly briefings on the state of Cybersecurity, Key Performance Indicators, and ongoing Cyber defensive technology projects.

"The Service Provider will inform the LIPA CIO of any significant breach or other unmitigated vulnerabilities immediately upon discovery."

- PSEG Long Island informed the LIPA CIO of all cyber incidents during 2021.

"LIPA will provide oversight, including review, Independent Verification, and Validation (IV&V) of the Services Provider's Cyber and Physical Security Program(s) as necessary."

- In 2022, LIPA will have a comprehensive vulnerability assessment, penetration testing, and overall cyber program evaluation conducted by an independent consultant. This assessment will include an independent review of PSEG Long Island's NIST CSF compliance status and will provide recommendations to achieve the target outlined in the reformed PSEG Long Island contract default metrics.

- In 2021, LIPA Staff conducted regularly scheduled meetings with PSEG Long Island's compliance group to review whether there were any issues requiring the need to self-report on any NERC standards. In 2022, LIPA will have a vulnerability assessment, and overall physical security program evaluation conducted by a third-party consultant/firm of critical infrastructure.

Annual Review of the Policy

At its meeting on November 17, 2021, the Board adopted a new policy on Information Technology and Cyber Security to replace this Policy. Moving forward, the annual reports to the Board will review compliance with the Board Policy on Information Technology and Cyber Security.

Recommendation

Based upon the foregoing, I recommend approval of the above requested action by adoption of a resolution in the form attached hereto.

Attachments

Exhibit "A" Resolution

Exhibit "A"

RESOLUTION RECOMMENDING APPROVAL OF THE ANNUAL REPORT TO THE BOARD OF TRUSTEES ON THE FORMER BOARD POLICY ON INFORMATION AND PHYSICAL SECURITY

WHEREAS, the Board Policy on Information and Physical Security (the "Policy") was originally approved by the Board of Trustees by Resolution No. 1500, December 18, 2019; and

WHEREAS, the Policy was last reviewed and amended by the Board at its meeting in December 2020; and

WHEREAS, the Oversight and Clean Energy Committee (the "Committee") of the Board of Trustees has conducted the annual review of the Policy and recommends that the Policy has been substantially complied with.

NOW, THEREFORE, BE IT RESOLVED, that consistent with the accompanying memorandum, the Committee hereby recommends that the Board find that LIPA has substantially complied with the Policy and approve the annual report to the Board.

Dated: December 15, 2021