BOARD AGENDA SUMMARY SHEET

Committee or Board:	**Date:**	**Board Meeting Date:**
Oversight and Clean Energy	December 11, 2020	December 16, 2020

***For All Board Voting Items*:**

Title of Agenda Item: Recommendation to Approve the Annual Report and Amendments to the Board Policy on Information and Physical Security

Consent Agenda: ☒Yes ☐No

Accompanying Presentation: ☐Yes ☒No

LIPA Presenter: Mujib Lodhi

PSEG Long Island Presenter: N/A

Enterprise Risk Management Discussion: ☐Yes ☒No

***For Policy Reports Only*:**

Type of Policy / Report: ☒ Operating; ☐ Governance; ☐ Compliance; ☐ Mission

Date of Last Report: N/A

Compliance Since Last Report: ☐Yes ☐No

Proposed Changes to Policy: ☒ Yes ☐No

Requested Action:	The Committee is requested to adopt a resolution recommending: (i) approval of the annual report on the Policy; (ii) that LIPA has complied with the Policy; and (iii) approval of certain amendments to the Policy.
Summary: **(include proposed amendments to Board Policies, if applicable)**	By Resolution No. 1500, dated December 18, 2019, the Board adopted the Policy. The Policy provides 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. LIPA Staff recommends that the Board find that LIPA has complied with the objectives of the Policy for the period since the initial adoption of the Policy. LIPA Staff also proposes to establish requirements for the Service Provider to: conduct vulnerability assessments and penetration testing and submit management action plans to LIPA; conduct an annual Cyber Security Maturity Assessment and self-assessment for NERC compliance and submit a management action plan to LIPA; and develop 3-Year Cyber and Physical security Strategic Plan and submit detailed annual Work Plan to LIPA.

FOR CONSIDERATION
December 16, 2020

TO: The Oversight and Clean Energy Committee

FROM: Thomas Falcone

SUBJECT: Recommendation to Approve the Annual Report and Amendments to the Board Policy on Information and Physical Security

---

Requested Action

The Oversight and Clean Energy Committee (the "Committee") of the 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 Board Policy on Information and Physical Security (the "Policy") (ii) that LIPA has complied with the Policy; and (iii) approval of certain amendments to 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 provides 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.

Compliance with the Policy

Staff recommends that, for the reasons set forth below, the Board find that LIPA has 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 maturity of the information and physical security programs of LIPA and its Service Provider, consistent with industry best practices."

- LIPA and its service providers, PSEG Long Island, have adopted the NIST Cybersecurity Framework (CSF) as part of their cybersecurity program. 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.

- PSEG Long Island -- Cybersecurity: PSEG engaged an outside consultant to perform an independent assessment of its enterprise Cybersecurity program and identified remediation plans to be implemented over the next three years.

- 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. A "Red Team" penetration test is conducted to assess the Security Command Center response.

- LIPA -- Cybersecurity: LIPA conducted a comprehensive third-party review of its cybersecurity program, including vulnerability assessment and penetration testing. Remediation plans were developed and are being implemented. Significant improvements in the LIPA's Cybersecurity management practices were made in 2020. However, we recognized the need to examine information security issues from a strategic perspective and address them in an organized manner; thus, an Information Security Strategic Plan will be developed to guide the protection of LIPA's information assets.

- Risk Management: The Board has adopted a policy on Enterprise Risk Management ("ERM"). Enterprise risks are brought to the Board's attention throughout the year. There are several risks identified related to Cyber and Physical security:
  - Cyber Event - "Unauthorized access to IT and/or T&D systems could result in decreased operational abilities".
  - Breach of Personal Identifiable Information ("PII") - "Internal or 3rd party mass-breach of PII could result in loss of sensitive data and potential fraud".
  - Physical Security Attack – "Substation security and the control centers are compromised and could result in reduced reliability".

  The Cybersecurity, PII, and physical security risks were all rated as medium level risks. Mitigation actions were identified to reduce business risks and negative impact on LIPA's assets.

"Compliance 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."

- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of requirements designed to secure the assets required for operating North

America's bulk electric system. Every three years, the Northeast Power Coordinating Council (NPPC) perform an audit for compliance. The last audit was conducted in 2018, and no issues were identified. The next compliance audit is scheduled for the first quarter of 2021. Recognizing the critical role of people to cybersecurity PSEG Long Island has undertaken various training and awareness initiatives in its efforts to stay compliant:

- Annual Cybersecurity training
- Cybersecurity awareness messages throughout the year
- Quarterly NERC CIP Awareness messages
- Quarterly Entitlement Reviews

"The Service Provider will immediately notify LIPA's Chief Information Officer of security breaches or attempted breaches and will confidentially report no less than quarterly to LIPA's Chief Information Officer on compliance with industry and regulatory standards and implementation of innovative defensive technology initiatives."

- In compliance with this policy requirement, PSEG Long Island staff provided periodic briefings on the state of Cybersecurity. Historically LIPA relied on PSEG Long Island representation. In 2021, LIPA plans to conduct a comprehensive review of the PSEG Long Island's cybersecurity program and its effectiveness.

Annual Review of the Policy

As shown in **Exhibit "B"**, LIPA Staff proposes to establish requirements for the Service Provider to:

- Conduct vulnerability assessments and penetration testing and submit management action plans to LIPA;
- Conduct an annual Cyber Security Maturity Assessment and self-assessment for NERC compliance and submit a management action plan to LIPA;
- Develop 3-Year Cybers and Physical security Strategic Plan and submit detailed annual Work Plan to LIPA.

These requirements will enhance LIPA's oversight of the requirements of this Policy.

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 "B" Board Policy on Information and Physical Security (redline)
Exhibit "C" Board Policy on Information and Physical Security (clean)

Exhibit "A"

RESOLUTION RECOMMENDING APPROVAL OF THE REPORT TO THE BOARD OF TRUSTEES ON THE 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 Oversight and Clean Energy Committee (the "Committee") of the Board of Trustees affirms that the Policy has been complied with and that the changes to the Policy recommended herein are due and proper.

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

BE IT FURTHER RESOLVED, that consistent with the accompanying memorandum, the Committee hereby recommends the changes to the Policy that are reflected in attachment **Exhibit "B"** are hereby approved.

Dated: December 16, 2020

Exhibit "B"

Board Policy:	**Cyber and Physical Security**
Policy Type:	**Operating Policies**
Monitored by:	**Oversight and ~~REV~~ Clean Energy Committee**
Board Resolution:	**#1500, approved December 18, 2019** **[#xxxx], amended December 16, 2020**

It is the policy of the Long Island Power Authority to maintain robust information management and physical security practices for its systems and assets, including those managed by its Service Provider. LIPA and its Service Provider will take prudent and reasonable measures to accomplish:

- **Information Security.** LIPA and its Service Provider will protect customer, employee and third-party information and LIPA information systems from unauthorized access or disruption.

- **Physical Security.** LIPA and its Service Provider will safeguard its employees while at work as well as its customers and visitors to LIPA facilities. LIPA and its Service Provider will also protect its facilities and functions that support the reliability of the electric system and its operations from unauthorized access or disruption of business operations.

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 ~~for such a review~~;

- 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 v~~V~~ulnerability 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;

- 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;

- The Service Provider will develop initial 3-Year Cyber and Physical Security Strategic P~~p~~lans and submit them~~it~~ to LIPA by July 2021;

- ~~T~~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;

- The Service Provider will develop and submit to LIPA ~~the~~an annual work~~-~~ plan in Q3 of each year for the subsequent year, guided by the Cyber and Physical Security Strategic Plans;

- The Service Provider shall ~~Compliance~~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

- 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

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

- LIPA will provide oversight, including review, ~~I~~independent verification, and validation (IV&V) of the Services Provider's Cyber and Physical Security Program(s) as necessary.

The Chief Executive Officer will report annually to the Board on compliance with the key provisions of this Policy.

Exhibit "C"

Board Policy:	**Cyber and Physical Security**
Policy Type:	**Operating Policies**
Monitored by:	**Oversight and Clean Energy Committee**
Board Resolution:	**#1500, approved December 18, 2019** **[#xxxx], amended December 16, 2020**

It is the policy of the Long Island Power Authority to maintain robust information management and physical security practices for its systems and assets, including those managed by its Service Provider. LIPA and its Service Provider will take prudent and reasonable measures to accomplish:

- **Information Security.** LIPA and its Service Provider will protect customer, employee and third-party information and LIPA information systems from unauthorized access or disruption.

- **Physical Security.** LIPA and its Service Provider will safeguard its employees while at work as well as its customers and visitors to LIPA facilities. LIPA and its Service Provider will also protect its facilities and functions that support the reliability of the electric system and its operations from unauthorized access or disruption of business operations.

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;

- 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;

- 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;

- 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;

- 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;

- 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.

- 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.

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

- 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.

The Chief Executive Officer will report annually to the Board on compliance with the key provisions of this Policy.