Briefing on Board Policy on Information Technology and Cyber Security

Presented by: Greg Flay, Chief Information Officer
Prepared for: LIPA Board of Trustees

December 17, 2025

Discussion Topics

- Board Policy Objectives
- Key Information Technology Projects

Board Policy Objectives

Information Technology Board Policy Objectives

Policy Component	Metric/Initiative
Invest in information technology that supports the **efficiency of business operations, promotes innovation, and provides long-term customer value**	• Substantial portfolio of IT projects to advance policy objective • IT-05 and IT-06 Project Performance metrics • IT-03 and IT-10 System Resiliency • IT-07 System Segregation
Deploy **modern grid management technology** and data analytics that enhance grid operations, customer service, utility asset management, and demand management, as measured by a Smart Grid Maturity Model level consistent with industry best practices	• Continue investments to implement and enable the planned expansions of smart grid technologies. • Perform a Smart Grid Maturity Model assessment in 2026
Ensure the **capacity of the information technology organization** to deliver reliable, robust, and resilient systems, as measured by a Capability Maturity Model Integration level of 3 or higher	• Perform regular CMMI assessments • IT-05 and IT-06 Project Performance metrics • Updated IT-06 performance metric which incentivizes on-time, on-budget project delivery with full scope and high quality
Regularly upgrade information and operational technology systems to **maintain all systems within their active service life and under general support** from the product vendor	• IT-04 System and Software Lifecycle Management metric

Cybersecurity and Data Privacy Board Policy Objectives

Policy Component	Metric/Initiative
Conduct quarterly internal vulnerability assessments and annual third-party vulnerability assessments and penetration testing of all information and operational technology systems and promptly mitigate vulnerabilities	• Monthly internal vulnerability assessments • Continuous cybersecurity posture monitoring via third-party • Annual penetration testing
Maintain a level of 3 or higher on the NIST Cybersecurity Framework, as evaluated annually through an independent assessment	• Annual assessments on NIST CSF • Next PSEGLI assessment scheduled for January 2026
Communicate how customer information is collected, used, and disclosed and ensure that, if confidential customer information is shared with a third-party for a business purpose, the third-party has robust information security practices	• FedRAMP and SOC-2 attestations • Third-party risk management program

Key Information Technology Projects

Information Technology Board Policy – Key IT Projects

Project	Purpose and Customer Benefits	Status and Plans
Systems Separation	**Separating all PSEG Long Island IT Systems serving LIPA from PSEG New Jersey systems.** ➢ Support efficient business operations ➢ Enhance grid operations ➢ Provide long-term customer value	• 98% complete. The last project is scheduled for completion in Dec 2025.
ADMS Network Model and Roadmap	**Builds on the Distribution SCADA platform, which went live in March 2020, and will develop a plan for the implementation of more advanced ADMS modules, such as FLISR.** ➢ Enhance grid operations ➢ Support efficient business operations ➢ Minimize operating costs ➢ Promote innovation	• Originally planned to start in Mar 2025 • Roadmap vendor has been selected and is currently onboarding • Will encompass people, process, technology, and facilities
CIS Replacement	**Replacement of 1970's-era mainframe customer system with a modern customer platform** ➢ Support efficient business operations ➢ Minimize operating costs ➢ Enhance grid operations ➢ Provide long-term customer value	• Sourcing vendor selected • Currently developing project scope • Platform and implementation partner selection in 2026

Information Technology Board Policy – Key IT Projects

Project	Purpose and Customer Benefits	Status and Plans
GRC (Governance, Risk, and Compliance) Tool Deployment	**Manage and automate GRC-related data and processes for Cyber Security, Business Continuity, and Disaster Recovery** ➢ Support efficient business operations ➢ Minimize operating costs ➢ Manage IT/OT system vulnerabilities ➢ Promptly mitigate vulnerabilities ➢ Maintain NIST CSF Level 3 ➢ Provide long-term customer value	• Delays due to onboarding resources and VDI technical issues. • In-service date has been moved from Dec 2025 to Feb 2026. • Scope and intended usage of BC/DR implementation needs to be better defined.
Standardized Data Access Platform	**Improve access to PSEG Long Island financial and operational data** ➢ Support efficient business operations ➢ Minimize operating costs ➢ Promote innovation	• Implemented Starburst technology to allow for direct LIPA access to the PSEGLI data lake • Implementing joint LIPA / PSEG-LI executive committee to review and prioritize data access and analytics requests to improve alignment

Information Technology Board Policy – Key IT Projects

Project	Purpose and Customer Benefits	Status and Plans
Customer Insights and Home Energy Management	**Consolidate home energy management portals to a single vendor and enhance the functionality of the remaining portal** ➢ Support efficient business operations ➢ Minimize operating costs ➢ Promote innovation	• Complete
CG Concentrator Replacement	**The new concentrators mitigate the risks related to smart device growth, product obsolescence, and cybersecurity risks** ➢ Support efficient business operations ➢ Minimize operating costs ➢ Enhance grid operations	• Complete
JMUX Replacement	**Implement a new technology platform to replace the nearing end-of-life network communication platform for critical T&D and NERC applications** ➢ Enhance grid operations ➢ Maintain vendor-supported systems	• Equipment vendor selection in Q4 2024 • Deployment 2025-2027
EMS Upgrade	**Upgrade the existing SCADA/EMS system** ➢ Enhance grid operations ➢ Maintain vendor-supported systems	• Delayed due to vendor resource availability. Currently planned for completion in April 2026.

Questions?

Greg Flay,
Chief Information Officer

lipower.org

FOR CONSIDERATION
December 17, 2025

TO: The Board of Trustees

FROM: Carrie Meek Gallagher

SUBJECT: Consideration of Approval of the Annual Report on the Board Policy on Information Technology and Cyber Security

---

Requested Action

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

Discussion

In December 2019, the Board adopted the Information and Physical Security Policy. The Policy delineated the Board's expectations and direction for information and physical security in accordance with public safety, operational, reputational, and compliance requirements. It established a reporting requirement to the Board on compliance with the key provisions of the Policy. In 2021, the prior policy was supplanted by the Information Technology and Cybersecurity Policy. The Policy provides that LIPA's "vision for information technology and cyber security is to use technology to enhance and simplify the customer experience, improve reliability, and minimize operating costs while ensuring robust, secure technology platforms that provide operational stability and protect customer, employee, and third-party data from unauthorized access or disruption. LIPA supports data privacy by transparently communicating how customer information is collected, used, and disclosed." The Board completed the last annual review of the Policy in December 2022.

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 since the last review.

Compliance with each element of the Policy is discussed in detail below.

1. "Invest in information technology that supports the efficiency of business operations, promotes innovation, and provides long-term customer value."
    - LIPA funded a substantial portfolio of IT projects in 2025, which advances the goals of increasing efficiency, promoting innovation, and providing long-term customer value. The

portfolio covers a range of projects, including enhancements to existing systems and implementation of new technologies, with the larger projects covered by the 2024 IT metrics. Some noteworthy IT projects are discussed below.

- System Separation: In the amended OSA between LIPA and PSEG Long Island, effective April 1, 2022, the parties agreed that it would be beneficial for all IT Systems serving LIPA to be separated and distinct from the systems, data, reports, and information of PSEG Long Island and its affiliates. The board-approved plan organizes the systems into four logical "bundles" for phased implementation. Work began on the first bundle in the last quarter of 2022 but has experienced significant schedule delays. However, the 2025 IT-07 System Separation metric is on schedule to be met. All systems are targeted to be separated by the end of 2025, in accordance with the OSA, and LIPA will continue to engage in oversight actively.
- Standardized Data Access Platform (SDAP): The SDAP project was initiated to implement the Board recommendation to improve LIPA and Department of Public Service ("DPS") access to PSEG Long Island financial and operational data through a Standardized Data Access Platform comprised of an enterprise-wide data warehouse, a broader data lake, and tools to support reporting and analytics. This past year has seen the implementation of the Starburst interface, which allows LIPA staff more direct access to the data lake than was previously available.
- CIS Replacement: PSEG Long Island has been using their existing customer information system (CIS) platform since the mid-1970's. While the underlying hardware and operating systems have been maintained at current levels, the application software is unable to meet current billing and customer needs, necessitating the use of ancillary systems like GridX for billing. The planning phase of the project has begun with the selection of a sourcing partner, who will in turn assist PSEG Long Island in the development of requirements and RFPs for the CIS product to be implemented as well as the system integration partner.
- Governance, Risk, and Compliance (GRC) Tool Deployment: This project will select and implement a GRC tool to manage and automate GRC-related data and processes for the critical areas of Cyber Security, Business Continuity, and Disaster Recovery. The tool will provide efficiencies through automation, support regulatory compliance, and enable the organization to mature risk management capabilities through data and process enhancements. The project was initiated in response to the 2023 NIST Cybersecurity Framework (CSF) assessment recommendation. Phase 0 will be completed in 2024, and it will provide vendor selection and a project plan for implementation in 2025.

- LIPA has also established annually recurring IT System Resiliency metrics (IT-03 and IT-10), which aim to minimize the probability and impact of system failures through well-designed, robust, and thoroughly exercised Disaster Recovery Plans (DRPs) and Business Continuity Plans (BCPs) for critical systems and processes. The IT-03 and IT-10 metrics were not met in 2022, 2023, or 2024. LIPA engaged a third-party consultant in 2024 to conduct a holistic assessment of the resiliency program and develop recommendations on

the path forward, including action plans with prioritized and achievable improvements. The assessment report was provided to PSEG Long Island in September 2024. The IT-03 metric was not properly funded for execution in 2025 and will not be met. The IT-10 metric was funded for 2025 and is expected to be met for 2025. Work on both efforts will continue into 2026.

2. "Deploy modern grid management technology and data analytics that enhance grid operations, customer service, utility asset management, and demand management, as measured by a Smart Grid Maturity Model level consistent with industry best practices (i.e., top 25% of utilities)."
   - The Smart Grid Maturity Model (SGMM) is a business tool stewarded by the Software Engineering Institute at Carnegie Mellon University. The model provides a framework for understanding the current extent of smart grid deployment and capability within an electric utility, a context for establishing strategic objectives and implementing plans that support grid modernization, and a means to evaluate progress over time toward those objectives. In 2022, LIPA engaged a consultant to conduct a smart grid maturity assessment using the Department of Energy's Next Generation Distribution System Platform (DSPx) reference from the Modern Distribution Grid Project, which is similar in content and format to the SGMM. The DSPx assessment recommended numerous areas for technology investment, such as Advanced Metering Infrastructure (AMI), Distributed Energy Resources Management Systems (DERMS), and Advanced Distribution Management System (ADMS). Several initiatives have since been undertaken, including AMI, DERMS, and the ADMS Roadmap.

3. "Ensure the capacity of the information technology organization to deliver reliable, robust, and resilient systems, as measured by a Capability Maturity Model Integration level of 3 or higher."
   - LIPA has established an Organizational Maturity metric to improve IT capability and performance and achieve Capability Maturity Model Integration (CMMI) Maturity Level 3. LIPA conducted a CMMI assessment in 2025 and determined that PSEG Long Island was operating at Level 3, as required.
   - LIPA has established the Project Performance metrics (IT-05 and IT-06) to improve project performance across the portfolio. In 2025, IT-05 is tracking 12 continuing projects, of which 8 are complete. Meanwhile, IT-06 is tracking 8 new projects for 2025, none of which have been completed. The use of metric exceptions to extend due dates for identified deliverables is extensive, which is why LIPA has developed an enhanced IT-06 metric for 2026. This metric provides an incentive for projects delivered on time, on budget, with full scope, and of high quality.

4. "Regularly upgrade information and operational technology systems to maintain all systems within their active service life and under general support from the product vendor."
   - Metric IT-04, System and Software Lifecycle Management was established to ensure all IT and OT assets managed by PSEG Long Island on behalf of LIPA, including but not limited to computers, communications equipment, networking equipment, hardware,

software, and storage systems, are within their active service life and under general support from the product vendor Pursuant to the metric, PSEG Long Island developed an Asset Inventory and a Two-Year Refresh Plan in 2022, which are now refreshed annually. The updated 2024-2025 Refresh Plan specifies a number of refresh projects to be conducted in 2024 to advance the objective of replacing or upgrading all end-of-life assets and was approved by LIPA. Execution of the plan is in progress.

- In 2024, the Life Cycle Replacement projects include some critical upgrades of operational technology systems, including:
    - EMS Upgrade: This project was initiated in 2024 to upgrade the SCADA/EMS system, add a test/development environment at the Alternate Control Center (ACC), and develop a solution for compliance with the Ambient Adjusted Rating regulatory requirement (FERC 841 Order). The project is currently scheduled to deploy the upgraded EMS (Energy Management System) at the current Transmission Control Center (TCC) and the ACC in May 2026.
    - JMUX Replacement: This multi-year project is for the evaluation, design, and implementation of a new technology platform to replace the nearing end-of-life Multiplexer, which provides the network communication platform for critical T&D and NERC applications. A Systems Integrator (SI) was selected in 2023 and conducted an RFP process for the evaluation and selection of a new equipment vendor, as well as design activities to assess the structural work required to accommodate the new equipment. The equipment vendor was selected in Q4 2024, with the implementation to continue through 2027.
    - CG Concentrator Project: The data Concentrators are critical networking devices that manage the communications and controls of over 3,000 SCADA devices across the PSEG Long Island service territory. The existing Concentrators had limited expansion capability and had come to the end of life for continued product support. In 2023, the project's first phase was completed with the selection of new Concentrators that provide the capacity needed to sustain the SCADA device growth as more Smart connected devices are connected to the grid, with enhanced cybersecurity features. Deployment was completed in 2025.
    - DER to DSCADA Communications Upgrade: This project upgrades the SCADA communications network from Distributed Energy Resources (DER) to the DSCADA/EMS systems and increases capacity, which is necessary to allow for new DER to be connected to the EMS and DSCADA systems at the currently projected growth rates. Deployment completed in 2025.

5. “Conduct quarterly internal vulnerability assessments and annual third-party vulnerability assessments and penetration testing of all information and operational technology systems and promptly mitigate vulnerabilities”

PSEG Long Island Cybersecurity

- Starting in late 2023, PSEG Long Island engaged an external vendor to conduct representative assessments of internal, external, D-SCADA, and mobile/web application attack surfaces. The results of these assessments were finalized in the summer of 2024. PSEG Long Island has reported that it has remediated all external surface vulnerabilities and the highest-severity internal vulnerabilities. Remediation is ongoing for the remaining vulnerabilities.
- As per the DPS Management Audit recommendation, LIPA is also conducting independent penetration testing and vulnerability assessment of the PSEG Long Island system. The vulnerability assessment and penetration testing for PSEG Long Island are scheduled to kick off in December 2025. The final assessment report is due in April 2026, and the final remediation report is expected in June 2026.
- Ransomware can severely impact business processes and leave organizations without the data to operate or deliver mission-critical services. The organizations affected often experience reputational damage, significant remediation costs, and interruptions in their ability to provide core services. In 2024, LIPA established the Ransomware Readiness and Response metric (IT-09). The metric ensures that any suspected or confirmed ransomware incidents are responded to consistently, controlled, and effectively. An independent third-party consultant reviewed and assessed the adequacy of PSEG Long Island's response to a ransomware incident. The assessment report was provided to PSEG Long Island in June 2024. The assessment report provided observations, identified gaps, and made recommendations. The recommendations are organized into an actionable roadmap based on best practices for developing, implementing, and improving PSEG Long Island's ransomware readiness and response plans. PSEG Long Island developed and submitted a PIP to LIPA for approval in 2025, aiming to fully implement the ransomware readiness and response roadmap, which aligns with the recommended timelines outlined in the assessment report. LIPA has engaged the services of an independent consultant to review the gap closure artifacts and deliverables, as well as the gap closure activities, and observe the ransomware response and recovery plan exercise, as required by the IT-09 performance metric. Gap closure is expected in 2026.

LIPA Cybersecurity

- In 2025, LIPA completed all information technology systems' third-party vulnerability assessments and penetration testing. The assessment vendor was engaged in April 2025, and the final assessment report was completed in August 2025. By mid-September 2025, LIPA had remediated all the vulnerabilities identified.
- LIPA's vulnerability management team meets weekly and reviews vulnerabilities identified in systems managed by LIPA using a real-time vulnerability management/reporting tool. The team creates the remediation plan for newly identified vulnerabilities based on their criticality and reviews the remediation status of previously identified vulnerabilities. LIPA has also implemented tools to provide 24x7 monitoring and notification of any new vulnerabilities identified. The vulnerability reporting tool sends daily alerts to the Cybersecurity team. Vulnerability management is reviewed monthly by the IT/cyber leadership.

6. “Maintain a level of 3 or higher on the NIST Cybersecurity Framework, as evaluated annually through an independent assessment.”
    - LIPA and PSEG Long Island have adopted the NIST Cybersecurity Framework (CSF) to improve cybersecurity programs. The Framework uses business drivers to guide cybersecurity activities. It considers cybersecurity risks as part of the risk management processes, including guidance on People, Processes, and Technology to implement defense in depth for the enterprise.
    - LIPA established a cybersecurity default metric for PSEG Long Island under the reformed PSEG Long Island contract, effective April 1, 2022, to achieve and maintain NIST CSF Tier 3. The reformed contract gives LIPA the right to terminate the contract should PSEG Long Island fail to maintain compliance, providing a strong improvement incentive. LIPA has hired a third-party evaluator to independently review PSEG Long Island's cyber readiness relative to the metric. The assessment work was completed in the First quarter of 2023, and the Final Assessment and Recommendations report was provided to PSEG Long Island in May 2023. A review by an independent consultant started in Q3 2024 to determine the progress PSEG Long Island has made to remediate the findings of the 2023 report. The final assessment report, delivered in December 2024, determined that PSEG-LI's cybersecurity program is predominantly operating at Tier 3 and provided recommendations for further strengthening cybersecurity controls. A follow-up NIST CSF assessment is planned for Q1 2026.
    - An independent assessment of LIPA’s cyber security posture using the NIST CSF was completed in Q4 2023. In Q1 2024, a work plan was developed to manage and track the implementation of the report's recommendations. LIPA completed the work identified in the work plan in July 2025.

7. “Communicate how customer information is collected, used, and disclosed and ensure that, if confidential customer information is shared with a third party for a business purpose, the third party has robust information security practices.”
    - PSEG Long Island collects customers’ information to provide electric service. The policy posted on the LIPA website describes what personal information is collected, when it is collected, how it is used, how it is protected, and under what circumstances that information may be shared with a third party. The policy has also been posted on the PSEG Long Island website.

Enterprise Risk Management Discussion

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 two high-priority risks related to the policy for both LIPA and PSEG Long Island. For both LIPA and PSEG Long Island, there is a risk of a cyber event resulting from unauthorized access to LIPA-managed systems that leads to material financial losses, impacts on LIPA’s day-to-day operations, or damage to the organization’s reputation. For PSEG Long Island, there is a risk of a major outage or performance failure of a critical operating technology or business system, resulting in extended disruption to operations or business processes, damage to systems, and/or loss of data. Also, the breach of

personally identifiable information (PII) could result in fraud, financial impact, and negative public perception.

LIPA's Department of Innovation and Information Technology mitigates these risks with a comprehensive risk management strategy and concurrent oversight of PSEG Long Island's IT department. The strategy includes several mitigation actions outlined in this memo, including the completion of annual penetration testing with remediation plans developed for identified vulnerabilities, the adoption of the NIST Cybersecurity Framework with the goal of maintaining a level 3 or higher assessment, and the implementation of a Cybersecurity Default Metric.

Considering the extensive efforts detailed in this Policy of both LIPA's Department of Innovation and Information Technology and PSEG Long Island's IT department, we believe the cyber and PII risks are being adequately managed.

Annual Review of the Policy

LIPA Staff has reviewed the Policy and recommends no change at this time.

Recommendation

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

Attachments

Exhibit "A" Resolution

Exhibit "A"

RESOLUTION APPROVING THE ANNUAL REPORT TO THE BOARD OF TRUSTEES ON THE BOARD POLICY ON INFORMATION TECHNOLOGY AND CYBER SECURITY

WHEREAS, the Board Policy on Information Technology and Cyber Security (the "Policy") was approved by the Board of Trustees (the "Board") of the Long Island Power Authority ("LIPA") in November 2021; and

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

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

Dated: December 17, 2025