GOVERNMENT OF PUERTO RICO
PUBLIC SERVICE REGULATORY BOARD
PUERTO RICO ENERGY BUREAU

IN RE: PUERTO RICO ELECTRIC POWER AUTHORITY RATE REVIEW	**CASE NO.:** NEPR-AP-2023-0003 **SUBJECT**: **Memorandum of Law in Support of Confidential Treatment of Portions of LUMA's Rate Review Petition**

MEMORANDUM OF LAW IN SUPPORT OF CONFIDENTIAL TREATMENT OF PORTIONS OF LUMA'S RATE REVIEW PETITION

TO THE HONORABLE PUERTO RICO ENERGY BUREAU:

COME NOW LUMA Energy, LLC ("ManagementCo"), and **LUMA Energy ServCo, LLC** ("ServCo"), (jointly referred to as "LUMA"), and respectfully state and request the following:

I. Introduction and Procedural Background

On June 30, 2024, this Honorable Puerto Rico Energy Bureau ("Energy Bureau") issued a Resolution and Order "to initiate [this] adjudicative process to review PREPA's rates" (the "June 30th Order) and opened this instant proceeding. *See* June 30th Order, p. 2.

Following a series of informal procedural events – including technical conferences and requests for information – aimed at receiving participants' respective insights and concerns with regards to the upcoming rate review petition, on February 12, 2025, this Energy Bureau issued a Resolution and Order ("February 12th Order"), whereby it established "the filing requirements and procedures for the rate review of the Puerto Rico Electric Power Authority ('PREPA')." *See* February 12th Order, p. 1.[1]

[1] Although not relevant to the present request, LUMA notes that the filing requirements issued by this Energy Bureau through its February 12th Order were later modified by way of orders issued on February 27, 2025, March 24, 2025, April 21, 2025, April 25, 2025, May 29, 2025 and, most recently, on June 11, 2025.

In what is pertinent to the present request, the February 12th Order established confidentiality "procedures to balance the public's right to access information about utility rates with the legitimate need to protect certain sensitive business information." *See* February 12th Order, p. 10. These mandate that, if in compliance with the February 12th Order, "a person has the duty to disclose to the Energy Bureau information that the person considers privileged under the Rules of Evidence, the person shall identify the information, request the Energy Bureau to protect the information, and provide written arguments to support its claim for protection,"[2] all as required by the Energy Bureau's Policy on Management of Confidential Information, CEPR-MI-2016-0009, issued on August 31, 2016, as amended on September 21, 2016 ("Policy on Confidential Information").

Furthermore, the February 12th Order states that the Energy Bureau will decide each confidentiality claim expeditiously and will proceed, in accordance with Article 6.15 of Act No. 57-2014[3], PR Laws Ann. Tit. 22 § 1054n (2025), 22 LPRA § 1054n (2025), if it deems that the protected material merits protection. *See* February 12th Order, p. 10. In its decision, "the Energy Bureau will state (i) which information and documents are confidential or privileged; and (ii) the rules that shall be observed to duly safeguard the information." *Id*. On the other hand, the February 12th Order provides the following:

> If the Energy Bureau denies a confidentiality claim, the Energy Bureau will also state the period after which the document or information will be available to the public. Such period will give the submitter sufficient time to seek reconsideration or any other legal recourse to prevent disclosure if PREPA disagrees with the Energy Bureau's decision.[4]

[2] *See* February 12th Order, p. 10.

[3] Known as the "Puerto Rico Energy Transformation and RELIEF Act" (hereinafter, "Act 57-2014").

[4] Lastly, the February 12th Order states that the "Energy Bureau's staff having access to Confidential Information will follow the *Puerto Rico Energy Bureau's Internal Guidelines for the Treatment of Confidential Information*." *See* February 12th Order, p. 10.

Id.

On July 3rd, 2025, LUMA filed its *Motion Submitting Rate Review Petition* ("Rate Review Petition"), in accordance with this Energy Bureau's February 12th Order, as subsequently amended. Together with its Rate Review Petition, LUMA filed a *Request for Confidential Treatment of Portions of LUMA's Rate Review Petition* ("Confidentiality Request"). Therein, LUMA submitted that very limited portions of the documents accompanying LUMA's Rate Review Petition contain confidential information that garner protection from public disclosure pursuant to applicable law and regulations. Accordingly, LUMA's Confidentiality Request identified the specific documents and portions for which confidentiality is sought[5] and informed the Energy Bureau that, in compliance with the Energy Bureau's Policy on Confidential Information, under separate cover and expediently, within the next ten (10) days, it would submit a memorandum of law in support of its request to file and maintain certain documents under seal of confidentiality.[6]

In compliance with the Energy Bureau's Policy on Confidential Information, LUMA hereby submits this memorandum of law that identifies and explains the legal basis for confidential treatment of portions of certain documents that were filed with this Energy Bureau together with the Rate Review Petition.

[5] *See* Section III of LUMA's Confidentiality Request.

[6] Moreover, pursuant to the Energy Bureau's Policy on Confidential Information, LUMA submitted redacted public versions of these documents, as well as confidential unredacted versions protecting the information deemed to be confidential.

II. Applicable Laws and Regulation to submit information confidentially before the Energy Bureau

Section 6.15 of Act 57-2014 regulates the management of confidential information filed before this Energy Bureau. It provides, in pertinent part, that: "[i]f any person who is required to submit information to the Energy [Bureau] believes that the information to be submitted has any confidentiality privilege, such person may request the Commission to treat such information as such . . . . " PR Laws Ann. Tit. 22 § 1054n (2025), 22 LPRA § 1054n (2025). If the Energy Bureau determines, after appropriate evaluation, that the information should be protected, "it shall grant such protection in a manner that least affects the public interest, transparency, and the rights of the parties involved in the administrative procedure in which the allegedly confidential document is submitted." *Id.*, Section 6.15(a).

In connection with the duties of electric power service companies, Section 1.10(i) of Act 17-2019[7] further provides that electric power service companies shall submit information requested by customers, except for: (i) confidential information in accordance with the Rules of Evidence of Puerto Rico. PR Laws Ann. Tit. 22 § 1141i (2025), 22 LPRA § 1141i (2025).

Access to the confidential information shall be provided "only to the lawyers and external consultants involved in the administrative process after the execution of a confidentiality agreement." Section 6.15(b) of Act 57-2014, PR Laws Ann. Tit. 22 § 1054n (2025), 22 LPRA § 1054n (2025). Finally, Act 57-2014 provides that this Energy Bureau "shall keep the documents submitted for its consideration out of public reach only in exceptional cases. In these cases, the information shall be duly safeguarded and delivered exclusively to the personnel of the [Energy Bureau] who needs to know such information under nondisclosure agreements. However, the

[7] Known as the "Puerto Rico Energy Public Policy Act" (hereinafter, "Act 17-2019").

[Energy Bureau] shall direct that a non-confidential copy be furnished for public review." *Id*., Section 6.15(c).

Moreover, the Energy Bureau's Policy on Confidential Information details the procedures that a party should follow to request that a document or portion thereof, be afforded confidential treatment. In essence, the Energy Bureau's Policy on Confidential Information requires identification of the confidential information and the filing of a memorandum of law, "no later than ten (10) days after filing of the Confidential Information," explaining the legal basis and support for a request to file information confidentially. *See* Policy on Confidential Information, Section A, as amended by the Resolution of September 16, 2016, CEPR-MI-2016-0009. The memorandum should also include a table that identifies the confidential information, a summary of the legal basis for the confidential designation and a summary of the reasons why each claim or designation conforms to the applicable legal basis of confidentiality. *Id*., paragraph 3. The party who seeks confidential treatment of information filed with the Energy Bureau must also file both "redacted" or "public version" and an "unredacted" or "confidential" version of the document that contains confidential information. *Id*., paragraph 6.

The Energy Bureau's Policy on Confidential Information also states the following with regards to access to Validated Confidential Information:

> […]
>
> 2. Critical Energy Infrastructure Information ("CEII")
>
> The information designated by the [Energy Bureau] as Validated Confidential Information on the ground of being CEII may be accessed by the parties' authorized representatives only after they have executed and delivered the Non-Disclosure Agreement.
>
> Those authorized representatives who have signed the Non-Disclosure Agreement may only review the documents validated as CEII at the [Energy Bureau] or the Producing Party's offices. During the review, the authorized representatives may

> not copy or disseminate the reviewed information and may bring no recording device to the viewing room.
>
> […]

Id., Section D (on Access to Validated Confidential Information).

Relatedly, Energy Bureau Regulation No. 8543, *Regulation on Adjudicative, Notice of Noncompliance, Rate Review, and Investigation Proceedings*, includes a provision for filing confidential information in adjudicatory proceedings before this honorable Energy Bureau. To wit, Section 1.15 provides that, "a person has the duty to disclose information to the [Energy Bureau] considered to be privileged pursuant to the Rules of Evidence, said person shall identify the allegedly privileged information, request the [Energy Bureau] the protection of said information, and provide supportive arguments, in writing, for a claim of information of privileged nature. The [Energy Bureau] shall evaluate the petition and, if it understands [that] the material merits protection, proceed according to . . . Article 6.15 of Act No. 57-2015, as amended."

III. Request for Confidentiality and Supporting Arguments

Act No. 40-2024, better known as the *Commonwealth of Puerto Rico Cybersecurity Act*, defines "Critical Infrastructure" ("Act 40-2024") as those "services, systems, resources, and essential assets, whether physical or virtual, the incapacity or destruction of which would have a debilitating impact on Puerto Rico's cybersecurity, health, economy, or any combination thereof." PR Laws Ann. Tit. 3 § 10124(p) (2024), 3 LPRA § 10124(p) (2024).[8] Generally, CEII or critical infrastructure

[8] With regards to Act 40-2024's applicability to LUMA, as Operator of the T&D System, said statute provides the following:

> The provisions of this chapter shall apply to the Executive Branch including all departments, boards, instrumentalities, commissions, bureaus, offices, agencies, administrations or bodies, political subdivisions, public corporations, and municipalities. **It shall likewise apply to every natural or juridical person doing business or having contracts with the Government including, but not limited to, private persons performing public services and duties**, but only with respect to the public services and duties being performed; any public or private administration exercise in which

information is exempted from public disclosure because it involves assets and information, which poses public security, economic, health, and safety risks. Federal Regulations on CEII, particularly, 18 C.F.R. § 388.113, states that:

> Critical energy infrastructure information means specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:
> (i) Relates details about the production, generation, transportation, transmission, or distribution of energy;
> (ii) Could be useful to a person in planning an attack on critical infrastructure;
> (iii) Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
> (iv) Does not simply give the general location of the critical infrastructure.

Id.

Additionally, "[c]ritical electric infrastructure means a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters." ***Id.*** Finally, "[c]ritical infrastructure means existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters." *Id.*

The Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 671-674 (2020), part of the Homeland Security Act of 2002, protects critical infrastructure information ("CII").[9] CII is

---

> public resources or funds were committed or invested (directly or indirectly), or in which any public servant exercised his authority with regards to the data collected as a result of such activities.

Section 2 of Act 40-2024, PR Laws Ann. Tit. 3 § 10122 (2024), 3 LPRA § 10122 (2024) (emphasis ours).

[9] Regarding protection of voluntary disclosures of critical infrastructure information, 6 U.S.C. § 673, provides in pertinent part, that CII:

> (A) shall be exempt from disclosure under the Freedom of Information Act;
> (B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;
> (C) shall not, without the written consent of the person or entity submitting such information, be used

defined as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems . . . ." 6 U.S.C. § 671 (3).[10]

As explained with particularity below, the portions of the Rate Review Petition that have been identified in Section IV of the present Motion – consisting of program briefs, fragments of prefiled testimony, and information provided in response to requests for information issued in sister dockets – include CEII, that is not common knowledge, is not made publicly available, and if

---

directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;
(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this part, except—
(i) in furtherance of an investigation or the prosecution of a criminal act; or
(ii) when disclosure of the information would be--
(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or
(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the Government Accountability Office;
(E) shall not, be provided to a State or local government or government agency; of information or records;
(i) be made available pursuant to any State or local law requiring disclosure of information or records;
(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or
(iii) be used other than for the purpose of protecting critical Infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.
(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

[10] CII includes the following types of information:

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, construction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

disclosed to the public, will expose key assets to security vulnerabilities or attacks by people seeking to cause harm to Puerto Rico's electric system. Therefore, it is in the public interest to keep the information confidential. For the reasons outlined below, confidential designation is a reasonable and necessary measure to protect critical infrastructure from attacks and to enable LUMA to leverage information without external threats.

i. Program Briefs

This honorable Energy Bureau has previously granted confidential treatment to all of the below identified program briefs, finding that the relevant portions included CEII that should be protected from disclosure. LUMA asks that the Energy Bureau follow its prior ruling and accept the relevant portions of the following programs confidentially. *See In Re*: *LUMA Initial Budgets and Related Terms of Service*, Case No. NEPR-MI-2021-0004.

a. LUMA Ex. 5.03 - OT Telecom Systems & Networks Program Brief (PBIT1) (FY2026)

This program includes Operational Technology ("OT") telecom investments to improve and revamp PREPA's mobile voice, transport network, fiber optic, and wireless data radio systems. These systems are used to carry out all of PREPA's ("IT") and OT data. They are, therefore, part of the critical infrastructure to operate the electrical grid safely and responsibly. The OT Telecom Systems & Networks Program Brief includes a description of the department's focus for FY2026-2028, with reference to the technology currently available for network connectivity and Telecom protection and the program for remediation, including the activities to be conducted. Additionally, the Program Brief identifies the active gaps within the program, which is a key component of protecting people, property and equipment. The aforementioned portions also reference cybersecurity vulnerabilities. Accordingly, all of this information should be kept confidentially, as

it involves critical infrastructure and provides LUMA's assessment of its vulnerabilities and how and why to address them with regards to the IT and OT Systems and Networks.

b. LUMA Ex. 11.02 - IT OT Cybersecurity Program Brief (PBIT2) (FY2026)

This program centers on enabling the business and protecting key organizational assets, including people, resources and technology to ensure that cyber risk, internal and external threats, vulnerabilities, and natural disasters are identified and mitigated based on risk and readiness factors. The IT OT Cybersecurity Program Brief includes descriptions of the program that identifies cyber risks that could severely impact T&D System operations.

Specifically, the IT OT Cybersecurity Program Brief provides content on the program for remediation, including the activities to be conducted and the types of security measures to be implemented. Additionally, the Program Brief describes primary goals, objectives and impact with reference to the benefits of the program, whilst identifying active gaps and risks of failing to implement adequate cybersecurity controls. These sections also reference cybersecurity vulnerabilities. All of this information should be kept confidentially, as it involves critical infrastructure and provides LUMA's assessment of its vulnerabilities and how and why to address them with regards to the IT and OT Systems and Networks. It bears noting that this Energy Bureau has kept pending proceedings on data security matters confidential. *See In re Review of the Puerto Rico Electric Power Authority Data Security Plan*, Case No. NEPR-MI-2020-0017.

c. LUMA Ex. 13.01 - Substation Physical Security Program Brief (PBUT18) (FY2026)

The Substation Physical Security Program focuses on a variety of security concerns at transmission and distribution substations which are critical to operate the Transmission and Distribution System ("System") and provide safe and reliable services. The Substation Security Program Brief provides content on the program for remediation, including the activities to be

conducted and the types of measures to be implemented to protect assets, employees and the public. Additionally, the Program Brief describes primary goals, objectives and impact with reference to the benefits of the program, whilst identifying active gaps and risks of failing to implement adequate security measures. This information should be kept confidential, as it involves critical infrastructure and provides LUMA's assessment on vulnerabilities and how to address them to provide security in distribution facilities. It bears noting that this Energy Bureau has conducted proceedings concerning physical security plan under strict confidentiality. *See In re Review of the Puerto Rico Electric Power Authority Physical Security Plan,* Case No. NEPR-MI-2020-0018.

d. LUMA Ex. 13.02 - Regional Operations Facilities Physical Security Program Brief (PBUT19) (FY2026)

The Regional Operations Facilities Physical Security Program focuses on replacing and adding new security technology and hardware to deter, detect and delay security incidents (e.g., intrusion, theft, damage) at Regional Operations facilities. Accordingly, the Regional Operations Facilities Physical Security Program Brief provides content on the program for remediation, including the activities to be conducted and the types of measures to be implemented to protect assets, employees and the public. Additionally, the Program Brief describes primary goals, objectives and impact with reference to the benefits of the program, whilst identifying active gaps and risks of failing to carry out this program. This information should be kept confidential, as it involves security at Regional Operations facilities and provides LUMA's assessment on vulnerabilities and how to address said vulnerabilities. It bears noting that this Energy Bureau has kept proceedings on physical security plan confidential. *See In re Review of the Puerto Rico Electric Power Authority Physical Security Plan,* Case No. NEPR-MI-2020-0018.

ii. *Testimony*

a. LUMA Ex. 11.0 - Direct Testimony of Crystal Allen, IT OT

LUMA Exhibit 11.0 contains detailed information regarding the design, operation, vulnerabilities, and security measures of Puerto Rico's electric transmission and distribution system. The above-identified pre-filed testimony outlines specific data security information,[11] descriptions of system gaps and vulnerabilities[12], levels of proposed funding and how it's distributed to combat said vulnerabilities[13], LUMA's cybersecurity practices and strategies[14], cybersecurity standards to which LUMA adheres to[15] and cybersecurity event statistics.[16] Additionally, LUMA Ex. 11.0 extensively outlines LUMA's IT OT Department's staffing needs.[17] LUMA's IT OT Department is responsible for the technology foundation that powers LUMA's grid operations, business functions, and cybersecurity defenses. Public disclosure of detailed staffing plans, including the number and allocation of cybersecurity personnel, would provide malicious actors with a roadmap to potential vulnerabilities in LUMA's organizational defenses. This could increase the risk of targeted cyberattacks, social engineering, or other security breaches aimed at exploiting perceived gaps in staffing or expertise.

---

[11] *See* Lines ("ll.") 370-371; 726-731; 743-747; 751-753; 758-760; 827; 853-854; 870-871; 875-876; 893-894; 1008; and 1216.

[12] *See* ll. 288-292; 295-302; 632-636; 645-647; 649; 707-715; 948-949; 989-993; 1008; 1014-1016; 1050-1062; 1181-1183; 1188-1191; 1206-1210; 1211-1213; and Table 1.

[13] *See* ll. 288-292; 582-587; 624-629; 668-671; 690-699; 707-715; 726-731; 735-739; 750-755; 763-766; 773-775; 781-783; 790-793; 853-855; 875-877; 893-895; 1160; 1179-1181; and Table 6 (except Totals).

[14] *See* ll. 150-165; 227-248; 589-621; 1173-1176; 1196-1199.

[15] *See* ll. 158-163; 232-233; 671-672; 674-675; 1181-1183.

[16] *See* ll. 227-229; 295-296; 300-302; 1166.

[17] *See* ll. 439; 440; 453; 454; 455; 461; 463; 471; 473; 480; 482; 486; 488; 492; 494; 498-504; 527; 528; Table 3 (except Totals); Table 4 (except Total); and Table 5 (except Totals).

Granting confidential treatment to the identified portions of this testimony is not only consistent with hallmark legal standards concerning CEII but is also fully consistent with, and in fact advances, Puerto Rico's public policy objectives as established by Act 40-2024. Section 3 of Act 40-2024[18] expressly mandates the protection and maintenance of the confidentiality, integrity,

[18] Section 3 of Act 40-2024 reads as follows:

> It is hereby established as the public policy of Puerto Rico:
>
> (1) To establish minimum cybersecurity standards and principles based on the "zero trust architecture" concept in order to enable the Government to incorporate cybernetic and electronic technologies into Government operations so as to transform and streamline intragovernmental relations, and government relations with the general public, as well as with local and foreign businesses, thus making the Government more accessible, effective, and transparent, in a secure and reliable manner.
>
> (2) To establish as policy that all covered agencies, or natural or juridical persons, as well as their agents, insurers, or guarantors are prohibited from making any ransom payments in response to a ransomware attack and that they shall collaborate with the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, as provided in the State and Local Government Cybersecurity Act of 2021. As an exception, and on a case-by-case basis, a Ransom Payment may be considered in the case of:
>
> (a) Critical infrastructure; or
> (b) Imminent risk of death;
> If a ransom payment is made due to any of the aforementioned reasons, upon consultation with the Office, it shall not be deemed a violation of this section.
>
> (3) To protect and maintain the confidentiality, integrity, and availability of the data stored and/or maintained by the Government's Information Resources and the related infrastructure assets, whether the data is at rest (stored), in-transit (being sent or received), or being created or transformed (processed).
>
> (4) To increase efforts to coordinate and improve the security of government networks and critical infrastructure as well as protect the data contained therein.
>
> (5) To enhance the capabilities and efforts to block, detect, prevent, protect from, and respond to threats against information resources and Government data.
>
> (6) To ensure a stable and secure Information Technology (IT) environment through the implementation of measures as are appropriate to mitigate cybersecurity risks by preventing, reducing, and limiting data loss or the degradation of the Government's information resources, and by implementing corrective measures and protocols that ensure that any imminent attack shall be addressed and resolved swiftly.
>
> (7) To protect the right to privacy of citizens without limiting their right to peaceful coexistence online.
>
> (8) To stop and punish persons misusing any type of information technology to commit criminal acts.

and availability of government data and related infrastructure assets, including those pertaining to critical infrastructure such as Puerto Rico's electric transmission and distribution system. Public disclosure of detailed cybersecurity information, including system vulnerabilities, security measures, and staffing allocations, would directly undermine these statutory objectives. Furthermore, Act 40-2024 emphasizes the need to implement minimum cybersecurity standards, coordinate security efforts, and ensure a stable and secure IT environment – goals that are only achievable if sensitive information is shielded from public exposure. Therefore, granting confidential treatment to this information is not only prudent but is also a legal imperative that aligns with the legislative intent to safeguard critical infrastructure, protect public safety, and comply with both local and federal cybersecurity requirements.

Disclosure of such information to the public would expose the electric grid to heightened risks of sabotage, cyberattacks, and other malicious acts, as it could be used by bad actors to plan and execute attacks on the system. Moreover, public disclosure of this information would undermine LUMA's ability to protect its assets, employees, and the public, and would contravene prudent utility practice as well as regulatory and contractual obligations under the *Transmission and Distribution System Operation and Maintenance Agreement* (T&D OMA).

The Energy Bureau has previously recognized the need to protect such information, granting confidential treatment to program briefs and cybersecurity plans containing similar

---

> (9) To comply with the basic cybersecurity guidelines established by the President of the United States, the Hon. Joe Biden, through the Executive Order issued on May 12, 2021, and with any subsequent orders related to cybersecurity.

PR Laws Ann. Tit. 3 § 10123 (2024), 3 LPRA § 10123 (2024).

information. Particularly, in proceedings related to Data Security[19] this Energy Bureau, *motu proprio,* has conducted proceedings – pertaining to subject matter closely aligned with the content of the testimony provided by way of LUMA Exhibit 11.0 – confidential, thereby recognizing the need to protect the above outlined CEII from public disclosure. The requested confidential treatment is essential to prevent the exposure of critical infrastructure to unnecessary risks and to comply with both federal and Puerto Rico law, as well as established regulatory policy, and should, thus, be granted accordingly.

iii. Other Supporting Documents

a. LUMA Exhibit 13.03 – Responses to Requests for Information issued on November 8, 2024 in Case No. NEPR-MI-2020-0018

On December 31, 2020, this Honorable Energy Bureau issued a Resolution and Order initiating Case No. NEPR-MI-2020-0018, *In re: Review of the Puerto Rico Electric Power Authority Physical Security Plan*, as a confidential proceeding to evaluate LUMA's Physical Security Plan. On May 28, 2021, LUMA filed its Physical Security Plan, developed pursuant to Section 4.2(h) of the T&D OMA, which was approved by the Energy Bureau on July 2, 2021.

As part of its monitoring of the Plan, on November 8, 2024, the Energy Bureau issued a Resolution and Order in Case No. NEPR-MI-2020-0018 ("November 8th Order"), in which it ordered LUMA to submit its answers to Requests of Information ("ROI") included in the Confidential Attachment A of the November 8th Order. In what is pertinent to the present motion, ROI #5 of the November 8th Order required LUMA to provide comprehensive data and analysis regarding its Physical Security, specifically focusing on security incidents, system performance, and staff training since January 2022. In compliance with the Energy Bureau's request, LUMA

[19] Case No. NEPR-MI-2020-0017, *In re Review of the Puerto Rico Electric Power Authority Data Security Plan*.

provided information regarding security incidents by type and location, by way of *ROI-LUMA-MI-2020-0018-20241108-PREB-005_Attachment20* and *ROI-LUMA-MI-2020-0018-20241108-PREB-005_Attachment21*.

LUMA's responses warrant confidential treatment because they contain information that falls squarely within the definitions of CEII and CII as established by applicable law. The information contained in LUMA's ROI responses includes, but is not limited to, incident logs, security incident trends, system uptime data, and descriptions of physical and cyber security controls – precisely the type of data that, if made public, could compromise the integrity of critical infrastructure. Granting confidential treatment is not only consistent with the applicable legal framework but is essential to safeguarding public safety, security, and the continued reliable operation of Puerto Rico's electric grid. It bears noting that this Energy Bureau has kept proceedings on the Physical Security Plan confidential and granted LUMA's request for confidential treatment of its responses to the November 8th Order.[20]

IV. Conclusion and Identification of Confidential Information within LUMA's Rate Review Petition

In conclusion, the aforementioned documents include information and programs for investments and remediation on critical infrastructure and components of PREPA systems whose function is to provide protection and security. They also involve critical elements of systems that are essential for LUMA's operations and critical communication components. If the information falls into the hands of people who may want to harm the T&D System, it will certainly provide

[20] In support of its request for confidential treatment, LUMA argued that maintaining confidentiality aids to protect the safety and integrity of the assets of the T&D System. LUMA explained that its responses to the November 8th ROIs contained CEII in the form of express coordinates to power transmission and distribution facilities of the T&D System, discussed express locations of security cameras and standard security operating procedures that garnered protection from public disclosures, pursuant to the applicable federal statutes and regulations on CEII. Moreover, LUMA reasoned that confidential designation is a reasonable and necessary measure to protect critical infrastructure from attacks and to enable LUMA to leverage information without external threats. Therefore, it was in the public interest to keep the information confidential.

sufficient details to expose the system to risks and harm. It is important to stress that information on security systems, per the aforementioned laws and regulations, should be shielded from public disclosure indefinitely to ensure the systems' integrity and functioning.

In compliance with the Energy Bureau's Policy on Confidential Information, CEPR-MI-2016-0009, an updated table summarizing the hallmarks of this request for confidential treatment is hereby included.

Document	Confidential Portions	Legal Basis for Confidentiality	Date Filed
LUMA Exhibit 5.03 – OT Telecom Systems and Networks Program Brief (PBIT1) (FY2026)	• Fiscal Year Focus 2026-2028 • Program Status • Active Gaps • Impact of Constrained Budget	Critical Energy Infrastructure Information 18 C.F.R. § 388.113; 6 U.S.C. §§ 671-674	July 3rd, 2025
LUMA Exhibit 11.00 – Direct Testimony of Crystal Allen, IT OT Testimony	• Lines ("ll.") 150-165; 227-248; 288-292; 295-302; 370-371; 439; 440; 453; 454; 455; 461; 463; 471; 473; 480; 482; 486; 488; 492; 494; 498; 499-504; 527; 528; 582-621; 624-629; 632-636; 645-647; 649; 668-672; 674-675; 690-699; 707-715; 726-731; 735-739; 743-747; 750-755; 758-760; 763-766; 773-776; 781-783; 790-793; 827; 853-855; 870; 871; 875-877; 893-895; 948-949; 989-993; 1008; 1014-1016; 1050-1062; 1160; 1166; 1173-1176; 1179-1183; 1188-1191; 1196-1199; 1206-1210; 1211-1213; 1216. • Table 1 • Table 3 (except Totals) • Table 4 (except Total) • Table 5 (except Totals) • Table 6 (except Totals)	Critical Energy Infrastructure Information 18 C.F.R. § 388.113; 6 U.S.C. §§ 671-674	July 3rd, 2025
LUMA Exhibit 11.02 – IT OT Cybersecurity Program Brief (PBIT2) (FY2026)	• Fiscal Year Focus 2026-2028 • Program Status • Active Gaps	Critical Energy Infrastructure Information 18 C.F.R. § 388.113; 6 U.S.C. §§ 671-674	July 3rd, 2025
LUMA Exhibit 13.01 – Substation Physical Security Program Brief (PBUT18) (FY2026)	• Fiscal Year Focus 2026-2028 • Program Status • Active Gaps • Impact of Constrained Budget	Critical Energy Infrastructure Information 18 C.F.R. § 388.113; 6 U.S.C. §§ 671-674	July 3rd, 2025

Document	Confidential Portions	Legal Basis for Confidentiality	Date Filed
LUMA Exhibit 13.02 – Regional Operations Facilities Physical Security Program Brief (PBUT19) (FY2026)	• Fiscal Year Focus 2026-2028 • Program Status • Active Gaps • Impact of Constrained Budget	Critical Energy Infrastructure Information 18 C.F.R. § 388.113; 6 U.S.C. §§ 671-674	July 3rd, 2025
LUMA Exhibit 13.03 – Response to November 8, 2024 Requests, Exhibit 1, ROI-LUMA-MI-2020-0018-20241108-PREB-005_Attachment20; and ROI-LUMA-MI-2020-0018-20241108-PREB-005_Attachment21 (Dec. 16, 2024)	Whole document(s).	Critical Energy Infrastructure Information 18 C.F.R. § 388.113; 6 U.S.C. §§ 671-674	July 3rd, 2025

WHEREFORE, LUMA respectfully requests that the Energy Bureau **take notice** of the aforementioned; and **grant** LUMA's request to keep the above-identified portions of the July 3rd Rate Review Petition under seal of confidentiality.

RESPECTFULLY SUBMITTED.

In San Juan, Puerto Rico, this 10th day of July, 2025.

WE HEREBY CERTIFY that this Motion was filed using the electronic filing system of this Energy Bureau and that electronic copies of this Motion will be notified to Hearing Examiner, Scott Hempling, shempling@scotthemplinglaw.com; and to the attorneys of the parties of record. To wit, to the ***Puerto Rico Electric Power Authority***, through: Mirelis Valle-Cancel, mvalle@gmlex.net; Juan González, jgonzalez@gmlex.net; Alexis G. Rivera Medina, arivera@gmlex.net; and Juan Martínez, jmartinez@gmlex.net; and to ***Genera PR, LLC***, through: Jorge Fernández-Reboredo, jfr@sbgblaw.com; Gabriela Castrodad, gcastrodad@sbgblaw.com; Jennise Alvarez, jennalvarez@sbgblaw.com; regulatory@genera-pr.com; José J. Díaz Alonso, jdiaz@sbgblaw.com; and legal@genera-pr.com; ***Co-counsel for Oficina Independiente de Protección al Consumidor***, hrivera@jrsp.pr.gov; contratistas@jrsp.pr.gov; pvazquez.oipc@avlawpr.com; ***Co-counsel for Instituto de Competitividad y Sustentabilidad Económica***, jpouroman@outlook.com; agraitfe@agraitlawpr.com; ***Co-counsel for National Public Finance Guarantee Corporation***, epo@amgprlaw.com; loliver@amgprlaw.com; acasellas@amgprlaw.com; matt.barr@weil.com; robert.berezin@weil.com; Gabriel.morgan@weil.com; Corey.Brady@weil.com; ***Co-counsel for GoldenTree Asset Management LP***, lramos@ramoscruzlegal.com; tlauria@whitecase.com; gkurtz@whitecase.com; ccolumbres@whitecase.com; iglassman@whitecase.com; tmacwright@whitecase.com; jcunningham@whitecase.com; mshepherd@whitecase.com; jgreen@whitecase.com; ***Co-counsel for Assured Guaranty, Inc.***, hburgos@cabprlaw.com; dperez@cabprlaw.com; mmcgill@gibsondunn.com; lshelfer@gibsondunn.com; howard.hawkins@cwt.com; mark.ellenberg@cwt.com; casey.servais@cwt.com; bill.natbony@cwt.com; thomas.curtin@cwt.com; ***Co-counsel for Syncora***

Guarantee, Inc., escalera@reichardescalera.com; arizmendis@reichardescalera.com; riverac@reichardescalera.com; susheelkirpalani@quinnemanuel.com; erickay@quinnemanuel.com; ***Co-Counsel for the PREPA Ad Hoc Group***, dmonserrate@msglawpr.com; fgierbolini@msglawpr.com; rschell@msglawpr.com; eric.brunstad@dechert.com; Stephen.zide@dechert.com; david.herman@dechert.com; michael.doluisio@dechert.com; stuart.steinberg@dechert.com; ***Sistema de Retiro de los Empleados de la Autoridad de Energía Eléctrica,*** nancy@emmanuelli.law; rafael.ortiz.mendoza@gmail.com; rolando@emmanuelli.law; ***Official Committee of Unsecured Creditors of PREPA***, jcasillas@cstlawpr.com; jnieves@cstlawpr.com; ***Solar and Energy Storage Association of Puerto Rico,*** Cfl@mcvpr.com; apc@mcvpr.com; javrua@sesapr.org; mrios@arroyorioslaw.com; ccordero@arroyorioslaw.com; ***Wal-Mart Puerto Rico, Inc.,*** Cfl@mcvpr.com; apc@mcvpr.com; ***Mr. Victor González,*** victorluisgonzalez@yahoo.com; and ***the Energy Bureau's Consultants,*** jrinconlopez@guidehouse.com; Josh.Llamas@fticonsulting.com; Anu.Sen@fticonsulting.com; Ellen.Smith@fticonsulting.com; Intisarul.Islam@weil.com; jorge@maxetaenergy.com; rafael@maxetaenergy.com; RSmithLA@aol.com; msdady@gmail.com; mcranston29@gmail.com; dawn.bisdorf@gmail.com; ahopkins@synapse-energy.com; clane@synapse-energy.com; guy@maxetaenergy.com; Julia@londoneconomics.com; Brian@londoneconomics.com; luke@londoneconomics.com; kbailey@acciongroup.com; hjudd@acciongroup.com; zachary.ming@ethree.com; PREBconsultants@acciongroup.com.

DLA Piper (Puerto Rico) LLC
Calle de la Tanca #500, Suite 401
San Juan, PR 00901-1969
Tel. 787-945-9122 / 9103
Fax 939-697-6092 / 6063

Margarita Mercado Echegaray
Margarita Mercado Echegaray
RUA 16,266
margarita.mercado@us.dlapiper.com

Jan M. Albino López
Jan M. Albino López
RUA 22,891
jan.albinolopez@us.dlapiper.com