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

IN RE: PUERTO RICO ELECTRIC POWER AUTHORITY'S EMERGENCY RESPONSE PLAN	**CASE NO.:** NEPR-MI-2019-0006 **SUBJECT:** Memorandum of Law in Support of Confidential Treatment of Genera's Updated Emergency Response Plan Submitted May 12, 2025

MEMORANDUM OF LAW IN SUPPORT OF CONFIDENTIAL TREATMENT OF GENERA'S UPDATED EMERGENCY RESPONSE PLAN SUBMITTED MAY 12, 2025

TO THE HONORABLE PUERTO RICO ENERGY BUREAU:

COMES NOW GENERA PR LLC ("Genera"), as agent of the Puerto Rico Electric Power Authority ("PREPA"),[1] through its counsels of record, and respectfully state and request the following:

I. Introduction

1. On August 16, 2023, the Energy Bureau of the Puerto Rico Public Service Regulatory Board ("Energy Bureau" or "PREB") issued a Resolution and Order titled *Filing of Emergency Response Plans ("ERP") – LUMA, Genera, and PREPA* ("August 16th Resolution") through which it acknowledged the Emergency Response Plans ("ERP") submitted by LUMA Energy, LLC and LUMA Energy Servco, LLC ("LUMA"), Genera, and PREPA; conditionally approved LUMA's ERP subject to specified requirements; rejected PREPA's ERP as filed; and

[1] Pursuant to the *Puerto Rico Thermal Generation Facilities Operation and Maintenance Agreement* ("LGA OMA"), dated January 24, 2023, executed by and among PREPA, Genera, and the Puerto Rico Public-Private Partnerships Authority, Genera is the sole operator and administrator of the Legacy Generation Assets (as defined in the LGA OMA) and the sole entity authorized to represent PREPA before PREB with respect to any matter related to the performance of any of the O&M Services provided by Genera under the LGA OMA.

noted that Genera's ERP was conditionally approved in a separate Resolution. Additionally, the Energy Bureau ordered LUMA, Genera, and PREPA to comply with certain specified requirements. Furthermore, the Energy Bureau established **December 15** as the annual deadline for filing ERPs, allowing adequate time to review, evaluate, and approve the ERPs before their required submission to the Governor and Legislature in accordance with Section 6(m) of Act No. 83 of May 2, 1941, as amended ("Act No. 83-1941").

2. On December 16, 2024, , Genera submitted its Emergency Response and Action Plan for year 2025 ("2025 ERP") and requested it be designated and kept as confidential.

3. On April 8, 2025, and May 5, 2025, Genera held meetings with PREB's consultants which resulted in the PREB requesting Genera submits an updated version of the 2025 ERP and the Fuel Purchase Agreements ("May 12 Motion").

4. In compliance with the Energy Bureau's request, on May 12, 2025, Genera filed a *Motion to Submit Genera PR LLC's Updated Emergency Response Plan and Fuel Purchase Agreements* submitting an updated version of the 2025 Emergency Response and Action Plan initially included with the May 12 Motion("Updated 2025 ERP"), and the Fuel Purchase Agreements filed as *Exhibits C, D, E,* and *F*. Furthermore, Genera claimed confidentiality for the Updated 2025 ERP, including the redline version ("Redlined Updated 2025 ERP"), submitted under seal as *Exhibits A* and *B*, respectively.

5. Genera informed the Energy Bureau that a Memorandum of Law would be submitted within the following ten days to support its request to maintain the confidentiality of the updated version of the ERP.

6.

II. Identification of Confidential Information

Document Name and File Date	Pages in which Confidential Information is Found, if applicable	Summary of Legal Basis for Confidential Designation, if applicable	Summary of why each claim or designation conforms to the applicable legal basis for confidentiality
Exhibit A Updated Emergency and Action Response Plan, filed on May 12, 2025.	N/A	Critical Energy Infrastructure Information under Section D(2) of the Energy Bureau's Policy on Confidential Information contained substantially and throughout the Updated 2025 ERP; and Critical Energy Infrastructure Information under 18 CFR § 388.113(c)(2) contained substantially and throughout the Updated 2025 ERP; Protection of sensitive personal information.	The importance of keeping sensitive national security protocols confidential is to prevent risks to employees, compromise of procedures, exploitation, or bypass by individuals with harmful intentions, unnecessary fear among the public, chaos, and strain on security resources. By maintaining confidentiality, real threats can be effectively responded to, potential misuse can be prevented, and public order can be maintained for the safety of the nation. The need for keeping sensitive critical energy infrastructure information is necessary for the orderly, effective and timely activation of the emergency response efforts by the relevant law enforcement and emergency response agencies and points of contact. The need to keep confidential certain telephone numbers in the presented documentation is necessary as a precautionary measure undertaken due to ambiguity regarding whether these numbers belong to private individuals or governmental agencies. Due diligence is

			actively being conducted to ascertain the nature and ownership of these numbers, in order to comply with legal and ethical standards concerning privacy and information disclosure.
Exhibit B Updated Redline version of Emergency and Action Response Plan, filed on May 12, 2025.	N/A	*See Id.*	*See Id.*

III. Memorandum of Law in Support of Confidential Treatment

A. Applicable Law

The governing statute for the management of classified information submitted to the Energy Bureau is Section 6.15 of Act No. 57-2014, also known as the "Puerto Rico Energy Transformation and RELIEF Act." This section stipulates that "[i]f any person who is required to submit information to the Energy [Bureau] believes that the information to be submitted carries a confidentiality privilege, such person may request the [Bureau] to treat such information as confidential…" 22 L.P.R.A. § 1054n. If, after conducting a meticulous evaluation, the Energy Bureau determines that the information warrants protection, it is required to "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*. at Section 6.15(a). Consequently, such information must be withheld from the public domain by the Energy Bureau and "must be duly safeguarded and provided exclusively to the personnel of the

Energy [Bureau] who need to know such information under nondisclosure agreements." *Id*. at Section 6.15(c). Therefore, "[t]he Energy [Bureau] must swiftly act on any privilege and confidentiality claim made by a person under its jurisdiction through a resolution for such purposes before any potentially confidential information is disclosed." *Id*. at Section 6.15(d).

Additionally, the Energy Bureau's Policy on Management of Confidential Information details the procedures a party should follow to request confidential treatment for a document or a portion of it. The Energy Bureau's Policy on Management of Confidential Information requires identifying confidential information and filing a memorandum of law explaining the legal basis and support for a request to file information confidentially. *See* Section A of the Energy Bureau's Policy on Management of Confidential Information. The memorandum should also include a table that identifies the confidential information, a summary of the legal basis for the confidential designation, and an explanation of why each claim or designation conforms to the applicable legal basis for confidentiality. *Id*. The party seeking confidential treatment of information filed with the Energy Bureau must also file both a "redacted" (or "public") version and an "unredacted" (or "confidential") version of the document that contains the confidential information. *Id*.

In addition to the above, Genera's updated Emergency Response & Action Plan encompasses Critical Energy Infrastructure Information ("CEII"). Federal statutes define CEII as:

> [S]pecific 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 ("FOIA"), 5 U.S.C. 552; and (iv) does not simply reveal the general location of the critical infrastructure."
>
> 18 CFR 388.113(c)(2).

Further, “critical electric infrastructure” is defined as “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 those matters." *Id.* §388.11(c)(4). As indicated, CEII is exempt from FOIA disclosure and must not be "made available by any Federal, State, political subdivision, or tribal authority under any Federal, State, political subdivision, or tribal law mandating public disclosure of information or records.” *Id*. §388.113(c)(1).

The Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 131-134 (“CII Act”), a component of the Homeland Security Act of 2002, provides additional protection to critical infrastructure information (“CII”), which is defined by statute as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems.” *See*, 6 U.S.C. § 133. With regards to the disclosure of such information, the Act specifies: “Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) voluntarily submitted to a covered federal agency for its use regarding the security of critical infrastructure and protected systems [...] (A) shall be exempt from disclosure under ... the Freedom of Information Act[ ]” and “(E) shall not, if provided to a state or local government or government agency, ... [ ] ... be made available pursuant to any state or local law requiring disclosure of information or records[.]” *Id*., § 133(a)(1)(A) & (E).

Regarding CEII, the Energy Bureau’s Policy on Management of Confidential Information stipulates that information designated by the Energy Bureau as validated Confidential Information on the grounds of being CEII may only be accessed by the parties' authorized representatives after they have executed and delivered a Non-Disclosure Agreement. *See* Section D(2) of the Energy Bureau’s Policy on Management of Confidential Information.

B. Ground for Confidentiality

Genera respectfully submits that the Updated 2025 ERP, included in Exhibit A of the May 12th 2025, Motion and detailed in Section II of this memorandum –including the Redlined Updated 2025 ERP submitted as Exhibit B for the exclusive purpose of aiding the PREB in its review of the Updated 2025 ERP– should be deemed confidential. In essence, Genera's Updated 2025 ERP, contains CEII, the confidentiality of which is crucial to ensuring both critical infrastructure security and public safety. While recognizing the Energy Bureau's commitment to transparency and public interest, Genera urges the Energy Bureau to consider the delicate balance between these commitments and the need for confidentiality in matters pertaining to critical infrastructure, all of which are cross-referenced, elaborated, and discussed substantially and throughout the Updated 2025 ERP. Disclosing the classified information contained within the Updated 2025 ERP would not only expose sensitive details but also jeopardize employee safety and compromise the integrity of specific operational procedures.

Additionally, there is a significant risk that individuals with malicious intent could access this sensitive infrastructure information, potentially exploiting or circumventing established protocols. Such inappropriate disclosures could incite public alarm and contribute to societal instability. Moreover, misuse or improper application of these procedures in non-emergency situations could provoke unnecessary disorder and strain Genera's security resources. Therefore, maintaining confidentiality is not only essential but wholly justified in the interests of national security and public welfare.

WHEREFORE, Genera respectfully requests that the Energy Bureau **take notice** of the above and **grant** this request for confidential treatment of the Updated 2025 ERP and the Redlined Updated 2025 ERP, filed on May 12, 2025, as *Exhibits A* and *B*.

RESPECTFULLY SUBMITTED.

In San Juan, Puerto Rico, this 22nd day of May of 2025.

ECIJA SBGB
PO Box 363068
San Juan, Puerto Rico 00920
Tel. (787) 300.3200
Fax (787) 300.3208

/s/ Jorge Fernández-Reboredo
Jorge Fernández-Reboredo
jfr@sbgblaw.com
TSPR 9,669

/s/ Stephen David Romero Valle
Stephen David Romero Valle
sromero@sbgblaw.com
RUA No. 21,881

/s/ Gabriela Alejandra Castrodad García
Gabriela Alejandra Castrodad García
gcastrodad@sbgblaw.com
TSPR 23,584

CERTIFICATE OF SERVICE

We hereby certify that a true and accurate copy of this motion was filed with the Office of the Clerk of the Energy Bureau using its Electronic Filing System and that we will send an electronic copy of this motion to arivera@gmlex.net; mvalle@gmlex.net; margarita.mercado@us.dlapiper.com; laura.rozas@us.dlapiper.com; Yahaira.delarosa@us.dlapiper.com; emmanuel.porrogonzalez@us.dlapiper.com; and nzayas@gmlex.net.

In San Juan, Puerto Rico, this 22nd day of May of 2025.

ECIJA SBGB
PO Box 363068
San Juan, Puerto Rico 00920
Tel. (787) 300-3200
Fax (787) 300-3208

/s/ Gabriela Alejandra Castrodad García
Gabriela Alejandra Castrodad García
gcastrodad@sbgblaw.com
TSPR 23,584