

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

NEPR
Received:
Jun 8, 2026
5:52 PM

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 Emergency
Response Plan

**MEMORANDUM OF LAW IN SUPPORT OF CONFIDENTIAL TREATMENT OF
GENERA'S EMERGENCY RESPONSE PLAN**

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 submits and prays as follows:

I. INTRODUCTION

1. On January 24, 2023, Genera, the Puerto Rico Electric Power Authority ("PREPA"), and the Puerto Rico Public-Private Partnership Authority ("P3A") entered into the Legacy Generation Assets Operation and Maintenance Agreement ("LGA OMA").

2. Section 4.2(e) of the LGA OMA requires Genera to:

[D]evelop in consultation with the T&D Operator and submit to Administrator and PREB, for their information and approval, a plan of action that takes effect from the Service Commencement Date and outlines the procedures and actions necessary for responding to any Emergency affecting or reasonably likely emergency that could affect the Legacy Generation Assets after the Service Commencement Date, including fire, weather, environmental, health, safety and other potential emergency conditions." The Legacy Generation Emergency Response Plan shall (i) provide for appropriate notice of any such emergency to T&D Operator, Administrator, PREB and all other Governmental Bodies that Operator is notified in writing have

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

jurisdiction of the Legacy Generation Assets, (ii) establish measures that facilitate coordinated emergency response actions by all appropriate Governmental Bodies, (iii) specifically include outage minimization and response measures and (iv) include measures designed to assure the timely availability of all personnel required to respond to any emergency in accordance with the Contract Standards.

3. Pursuant to Section 4.2(e) of the OMA, Genera must, in consultation with the T&D Operator, develop and submit a plan of action to P3A and the Energy Bureau for approval (the “Legacy Generation Emergency Response Plan” or “ERP”). This plan should outline the necessary procedures and actions to respond to emergencies that could affect the Legacy Generation Assets, including fire, weather, environment, health, safety, and other potential emergency conditions.

4. Section 4.2(e) of the OMA further outlines that the ERP should include a protocol for notifying relevant parties about an emergency; measures for facilitating coordinated emergency response actions; specific outage minimization and response measures; and provisions for ensuring the timely availability of all personnel required to respond to an emergency in line with the Contract Standards.

5. On August 16, 2023, the Puerto Rico Energy Bureau (“Energy Bureau”) issued a Resolution and Order titled *Filing of Emergency Response Plans (“ERP”) – LUMA, Genera, and PREPA* (“August 16th Resolution”) through which it acknowledged the proposed Emergency Response Plans (“ERP”) submitted by LUMA, Genera, and PREPA. Relevant to the instant motion, the August 16th Resolution established **December 15** as the annual deadline for filing ERPs, allowing adequate time to review, evaluate, and approve the ERPs before the required annual report to the Governor and Legislature in accordance with Section 6(m) of Act No. 83 of

May 2, 1941, as amended (“Act 83-1941”), which must be submitted on or before May 31 of each year².

6. In compliance with the Energy Bureau’s directives, on December 15, 2025, Genera submitted its Emergency Response & Action Plan for year 2026 for the Energy Bureau’s consideration and requested that it be treated as confidential.

7. Notwithstanding the foregoing, on May 29, 2026, following discussion with the Energy Bureau’s consultants, Genera submitted as Exhibit A to the *Motion to Submit Annual Report in Compliance with Section 6(m) of Act. No 83 of May 2, 1941, as amended* (the “May 29th Motion”), an updated version of its Emergency Response & Action Plan for year 2026 (“2026 ERP”). As such, Genera respectfully requested that it should be treated as confidential given that it includes critical infrastructure information

8. Genera informed the Energy Bureau that a Memorandum of Law would be submitted within the following ten (10) days to support its request to maintain the confidentiality of the updated version of the ERP. Pursuant to its *Policy on Management of Confidential*

² Pursuant to Section 6(m) of Act No. 83-1941, PREPA is required to:

To submit a report to the Governor, the [Energy] Bureau, and both Houses of the Legislative Assembly, not later than May 31 of every year, stating the measures taken during the preceding calendar year to address the emergencies that may arise with respect to the upcoming hurricane season and other atmospheric disturbances, including floods that may affect the electrical system of the Island. Likewise, said report shall present the adopted plans or protocols to be followed in case of fires in facilities and establishments of [PREPA]. It shall also include any preventive measure identified for the conservation of the power lines in the event of an earthquake. The report shall include, but not be limited to, the following information:

- i. Improvements to [PREPA’s] Revised Operating Plan for Emergencies due to Atmospheric Disturbances.
- ii. development of an emergency plan to face a possible earthquake.
- iii. Adopted plans or protocols to be followed in case of fire in [PREPA’s] facilities and establishments.
- iv. Status of the tree trimming program in order to protect power transmission lines, while protecting our trees and preventing them from being damaged;
- v. Decision-making protocol to enforce the shutting down of the electrical system;
- vi. Trainings offered to [PREPA]’s essential personnel to qualify it on the procedure to be followed in case of emergencies arising from atmospheric disturbances, fire in [PREPA]’s facilities or establishments, or earthquakes, as well as a certification attesting that all the personnel performing supervisory functions in the operating areas has been duly advised on the norms of the operating emergency plan in effect; and
- vii. Contingency plans to address the situation after a storm, a hurricane, a fire in [PREPA]’s facilities or establishments, or an earthquake, directed to normalizing or reestablishing the electrical system as soon as possible.

22 L.P.R.A. § 196(m)

Information, CEPR-MI-2016-0009 (“PREB’s Policy on Confidential Information”), as amended, Genera respectfully requests confidential designation of the 2026 ERP submitted herein, and submits the following Memorandum of Law.

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
<p>Exhibit A Updated Emergency Response Plan filed on May 29, 2026.</p>	<p>Whole document</p>	<p>Critical Energy Infrastructure Information under Section D(2) of the Energy Bureau’s Policy on Confidential Information contained substantially and throughout the Emergency Response Plan; and Critical Energy Infrastructure Information under 18 CFR § 388.113(c)(2) contained substantially and throughout the Updated 2026 ERP; Protection of sensitive personal information.</p>	<p>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.</p> <p>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.</p> <p>The need to keep confidential certain telephone numbers in the presented documentation is necessary as a</p>

			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.
--	--	--	--

III. MEMORANDUM OF LAW IN SUPPORT OF CONFIDENTIAL TREATMENT OF GENERA’S EMERGENCY RESPONSE PLAN

9. 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).

10. 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). 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.” *Id.* Section 6.15(b), 22 LPRA §1054n. 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). 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 [Energy Bureau] shall direct non-confidential copy be furnished for public review”. *Id.* Section 6.15(c).

11. 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.* With respect to access to validated Critical Energy Infrastructure Information (the “CEII”), the Policy further provides that the information designated by the Commission as Validated Confidential Information on the grounds 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 Commission or the Producing Party's offices. During said review, the authorized representatives may not copy or disseminate the reviewed information and may not bring any recording device to the viewing room. *Id.* Section D (2).

12. Relatedly, Energy Bureau Regulation 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 and 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 what is set forth in Articles 6.15 of Act No. 57-2014, as amended." Section 1.15, Confidential Information, Energy Bureau Regulation 8543, *Regulation on Adjudicative, Notice of Noncompliance, Rate Review, and Investigation proceedings*.

13. In addition to the above, Genera's Emergency Response 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).

14. 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 FOIA exemption most directly applicable to CEII is Exemption 3, which protects information withheld pursuant to a statute that establishes particular criteria for withholding. Both the Critical Infrastructure Information Act of 2002 and FERC’s CEII regulations under 18 CFR § 388.113 constitute such statutes, independently establishing the criteria under which this category of information must be withheld from public disclosure. The emergency response protocols, contact chains and operational procedures contained in Genera’s 2026 ERP fall within both exemptions, as their disclosure could enable targeted interference with generation assets and endanger the personnel responsible for emergency response operations.

15. The Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 671-674 (“CII Act”), a component of the Homeland Security Act of 2002, provides additional protection to critical infrastructure information (“CII”)³, which is defined by statute as “information not

³ Regarding protection of voluntary disclosures of critical infrastructure information, the CII Act state, in its pertinent part, that CII:
(A) shall be exempt from disclosure under section 552 of title 5 (commonly referred to as 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 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;

customarily in the public domain and related to the security of critical infrastructure or protected systems.” See, 6 U.S.C. § 650 (4)⁴. 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.*, § 673(a)(1)(A) & (E).

16. 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 Ric’s cybersecurity, health, economy, or any combined

-
- (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, if provided to a State or local government or government agency—
- (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; and
- (F)** does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

⁴ The term “critical infrastructure information” means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

- (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, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

thereof.” 3 LPRA § 10124p. With regards to Act 40-2024’s applicability to genera, as Operator of the O&M Services for the Legacy Generation Assets, said statute provide the following:

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

3 LPRA § 10122

17. Generally, CEII or critical infrastructure information is exempted from public disclosure because it involves assets and information that pose public security, economic, health and safety risks.

18. Genera, as the sole operator of the Legacy Generation Assets under the LGA OMA, constitutes a private entity performing public services and duties pursuant to a contract with the Government of Puerto Rico within the meaning of 3 LPRA § 10122. The 2026 ERP, which details emergency response protocols, personnel contact chains, and operational procedures for critical generation assets serving the island’s electrical grids, falls squarely within the critical infrastructure protection purposes of Act No. 40-2024. Accordingly, the information contained therein is entitled to the protection afforded by Act. No. 40-2024 to the same extent as information held by the public entities with which Genera coordinates its emergency response efforts.

19. 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.

20. In light of the above explained applicable law, Genera respectfully submits that the Emergency Response Plan, included as Exhibit A of the instant are protected from disclosure due to containing CII and CEII throughout which warrant confidential designation and treatment.

21. In essence, Genera's 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 ERP submitted herein. Disclosing the classified information contained in this ERP would not only expose sensitive infrastructure details but also jeopardize employee safety and compromise the integrity of specific operational procedures.

22. Furthermore, the 2026 ERP contains telephone numbers embedded within emergency contact chains that may belong to private individuals rather than governmental agencies. To the extent that any such numbers belong to private persons, their public disclosure could implicate privacy protections under the constitutional right to privacy recognized under Article II, Section 8 of the Constitution of the Commonwealth of Puerto Rico, as well as applicable federal privacy norms. As a precautionary measure, and pending completion of due diligence to ascertain the nature and ownership of each number, Genera respectfully submits

that confidential treatment of the ERP in its entirety is warranted to preserve the privacy interests of any private individuals whose contact information appears therein.

23. 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.

24. This honorable Energy Bureau has previously granted confidential treatment to information submitted by Genera under this same Policy framework, recognizing the legitimacy of Genera's confidentiality claims and the importance of protecting sensitive operational information from public disclosure. Consistent with that precedent, and in light of the compelling legal basis set forth herein, Genera respectfully submits that the 2026 ERP warrants the same treatment.

WHEREFORE, Genera respectfully requests that the Energy Bureau **take notice** of the above for all purposes; **GRANT confidential treatment** to Genera's 2026 Updated ERP submitted as Exhibit A to the May 29th Motion, pursuant to the Energy Bureau's *Policy on Management of Confidential Information*, CEPR-MI-2016-0009, as amended, and pursuant to the applicable law regarding confidentiality claims over Critical Infrastructure Information and Critical Energy Infrastructure Information; and **grant** any and all other relief that the Energy Bureau deems just and proper.

RESPECTFULLY SUBMITTED.

In San Juan, Puerto Rico, this 8th day of June of 2026.

ECIJA SBGB

PO Box 363068

San Juan, PR 00936-3068

Tel. (787) 300.3200

Fax (787) 300.3208

/s/ Jorge Fernández-Reboredo

Jorge Fernández-Reboredo

jfernandez@ecija.com

RUA No. 9,669

/s/ Ernesto Raúl Ramos Maldonado

Ernesto Raúl Ramos Maldonado

eramos@ecija.com

RUA No. 23,882

/s/ Gabriela Alejandra Castrodad García

Gabriela Alejandra Castrodad García

gcastrodad@ecija.com

RUA No. 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@prepa.pr.gov; mvalle@gmlex.net; margarita.mercado@us.dlapiper.com; laura.rozas@us.dlapiper.com; Yahaira.delarosa@us.dlapiper.com; emmanuel.porrogonzalez@us.dlapiper.com; gcastrodad@ecija.com; and nzayas@gmlex.net.

In San Juan, Puerto Rico, this 8th day of June of 2026.

/s/ Jorge Fernández-Reboredo
Jorge Fernández-Reboredo

/s/ Ernesto Raúl Ramos Maldonado
Ernesto Raúl Ramos Maldonado

/s/ Gabriela Alejandra Castrodad García
Gabriela Alejandra Castrodad García