NEPR

Received:

Aug 4, 2025

6:48 PM

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

IN RE: PUERTO RICO ELECTRIC POWER AUTHORITY RATE REVIEW

SUBJECT: Memorandum of Law in Support of Confidential Treatment of Portions of LUMA's Response to PREPA-of-LUMA-PROV-8

CASE NO.: NEPR-AP-2023-0003

MEMORANDUM OF LAW IN SUPPORT OF CONFIDENTIAL TREATMENT OF PORTIONS OF LUMA'S RESPONSE TO PREPA-OF-LUMA-PROV-8

TO THE HONORABLE PUERTO RICO ENERGY BUREAU AND ITS HEARING EXAMINER, SCOTT HEMPLING:

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

I. INTRODUCTION

- 1. LUMA respectfully submits this Memorandum of Law in support of its request for confidential treatment of specific portions of its response to the Puerto Rico Electric Power Authority's ("PREPA") Request for Information identified as PREPA-of-LUMA-PROV-8 ("PREPA ROI 8"). The information at issue, contained in PREPA-of-LUMA-PROV-8_ROI-PREPA-LUMA-PROV-8_Attachment 1 ("LUMA Attachment 1"), includes sensitive data related to LUMA's Information Technology ("IT"), Operational Technology ("OT"), and Cybersecurity programs and their implementation.
- 2. LUMA seeks confidential treatment of this information pursuant to the applicable legal and regulatory framework, including Section 6.15 of Act 57-2014,² PR Laws Ann. Tit. 22 §§

¹ The Accion platform automatically assigned the following code to the attachment Response_1753487752006_PREPA-of-LUMA-PROV-8_ROI-PREPA-LUMA-PROV-8_Attachment 1_

² Known as the "Puerto Rico Energy Transformation and RELIEF Act" and hereinafter referred to as Act 57-2014.

1051-1056, 22 LPRA §§ 1051-1056 (2025), the Energy Bureau's Policy on Confidential Information (CEPR-MI-2016-0009), and the Commonwealth of Puerto Rico Cybersecurity Act (Act 40-2024),³ PR Laws Ann. Tit. 3 §§ 10121 - 10135 (2025), 3 LPRA §§ 10121 - 10135 (2025). The redacted material qualifies as Critical Energy Infrastructure Information ("CEII") and, if publicly disclosed, could expose the electric grid to significant security risks, including cyberattacks and other malicious acts.

3. Accordingly, LUMA respectfully requests that the Puerto Rico Energy Bureau ("Energy Bureau") determine that the identified portions of LUMA Attachment 1, filed on July 25, 2025, in response to PREPA ROI 8, constitute Valid Confidential Information and order that such information be maintained under seal to safeguard Puerto Rico's critical energy infrastructure and ensure compliance with applicable law and public policy.

II. PROCEDURAL BACKGROUND

- 4. On June 30, 2024, this Honorable 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.
- 5. 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 [PREPA])." *See* February 12th Order, p. 1.4

³ Known as the "Commonwealth of Puerto Rico Cybersecurity Act" and hereinafter referred to as Act 40-2024.

⁴ 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.

- 6. 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," 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").
- 7. 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, 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.⁶

Id.

⁵ See February 12th Order, p. 10.

⁶ 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.

- 8. On July 10, 2025, PREPA submitted a request of information ("ROI") directed to LUMA under the Provisional Rate category. The identification code assigned by the Accion platform to said ROI is PREPA-of-LUMA-PROV-8.
- 9. On July 15, 2025, LUMA submitted an objection to PREPA's ROI. On July 18, 2025, the Hearing Examiner entered an order titled Order on LUMA's Objections to ROI #PREPA-of-LUMA-8, granting in part and denying in part LUMA's Objection to PREPA ROI 8. On July 21, 2025, the Hearing Examiner granted LUMA, with certain caveats, until July 25, 2025 to respond to those requests that were allowed. Per the February 12th 2025 Order, responses to ROIs are due at 5:00 pm.
- 10. After several procedural events, on July 25, 2025, LUMA presented a request for a three (3) hour extension to respond to PREPA ROI 8. PREPA did not respond to said request. Nonetheless, LUMA proceeded to submit the response on the same day.
- 11. LUMA's response was supported by two attachments. One of the attachments was a redacted Excel spreadsheet identified by LUMA as PREPA-of-LUMA-PROV-8_ROI-PREPA-LUMA-PROV-8_Attachment 1. The redactions made to LUMA Attachment 1 are intended to maintain confidentiality of certain portions of LUMA Attachment 1 that show information related to IT, OT and Cybersecurity.
- 12. Today, LUMA will submit revised redactions to LUMA Attachment 1 via the Accion platform. These revisions publish portions of the original response, resulting in fewer redactions than in the initial submission. For purposes of this memorandum, LUMA addresses the redactions reflected in today's revised version of LUMA Attachment 1.
- 13. In compliance with the procedures established in the Policy on Confidential Information, LUMA submits this memorandum of law to support its request for confidentiality,

asking the Energy Bureau to determine that LUMA Attachment 1 includes Valid Confidential Information and requesting that the unreducted version of LUMA Attachment 1 be maintained under seal of confidentiality by the Clerk of the Energy Bureau.

III. APPLICABLE LAW

- 14. 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).
- 15. In connection with the duties of electric power service companies, Section 1.10(i) of Act 17-2019⁷ 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).
- 16. 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

5

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

Bureau] who needs to know such information under nondisclosure agreements. However, the [Energy Bureau] shall direct that a non-confidential copy be furnished for public review." *Id.*, Section 6.15(c).

- 17. 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.
- 18. 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).

19. 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."

IV. DISCUSSION IN SUPPORT OF CONFIDENTIALITY REQUEST

20. Act No. 40-2024, better known as the *Commonwealth of Puerto Rico Cybersecurity Act*, defines "Critical Infrastructure" 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) (2025). 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 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.

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 (2025), 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.

- 21. 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.*
- 22. The Critical Infrastructure Information Act of 2002, 6 U.S.C. §§ 671-674 (2025), part of the Homeland Security Act of 2002, protects critical infrastructure information ("CII").

Section 2 of Act 40-2024, PR Laws Ann. Tit. 3 § 10122, 3 LPRA § 10122 (2025) (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 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;

CII is defined as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems" 6 U.S.C. § 650 (4) (2025); 6 U.S.C. § 671 (3).¹⁰

- (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.

6 U.S.C. § 650 (4).

⁽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—

As explained with particularity below, the portions of LUMA Attachment 1 that have been identified in subpart (IV.B) of this Memorandum, regarding costs of the IT, OT and Cybersecurity Department, are CEII and CII, that is not common knowledge, is not made publicly available, and if 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.

A. IT, OT and Cybersecurity Information in LUMA Attachment 1

- 24. LUMA Attachment 1 includes information pertaining to the Collaboration & Analytics, Cybersecurity, and Asset Management programs. The redacted portions contain descriptions of program implementation, including cost allocation for O&M and NFC, and names of the specific tools and software utilized for these sensitive programs.
- 25. Granting confidential treatment to the identified portions of LUMA Attachment 1 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 40-2024¹¹ expressly mandates the protection and maintenance of the

It is hereby established as the public policy of Puerto Rico:

¹¹ Section 3 of Act 40-2024 reads as follows:

⁽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.

confidentiality, integrity, 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 funding needs for Collaboration & Analytics, Cybersecurity, and Asset Management programs, based on needs which in turn reflect vulnerabilities, would directly undermine these statutory objectives. Act 40-2024 emphasizes the

(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.
- (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, 3 LPRA § 10123 (2025).

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. 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.

- 26. Disclosure 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 *Puerto Rico Transmission and Distribution System Operation and Maintenance Agreement* of June 22, 2022, as supplemented and amended by the *Puerto Rico Transmission and Distribution System Operation and Maintenance Supplemental Terms Agreement* ("T&D OMA").
- 27. The requested confidential treatment is justified 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.

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

28. The portions of LUMA Attachment 1 identified below contain sensitive technical information related to the Collaboration & Analytics, Cybersecurity, and Asset Management programs. These include descriptions of system requirements, operational tools used in the execution of O&M and NFC functions, and investment and remediation strategies targeting critical infrastructure and PREPA system components. The information further reveals elements integral

to LUMA's operational continuity and secure communications. Public disclosure of these details could compromise system integrity and security, and therefore warrants confidential treatment.

- 29. If the information falls into the hands of people who may want to harm the T&D System, it will certainly provide sufficient details to expose the system to risks and harm. It is important to stress that information on cybersecurity systems, per the aforementioned laws and regulations, should be shielded from public disclosure indefinitely to ensure the systems' integrity and functioning.
- 30. 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	Date Filed
		Confidentiality	
PREPA-of-LUMA-	Collaboration &	Critical Energy	July 25, 2025,
PROV-8_ROI-	Analytics, column	Infrastructure Information	and amended
PREPA-LUMA-	11	18 C.F.R. § 388.113; 6	on August 4,
PROV-	• Cybersecurity,	U.S.C. §§ 650 (4) (2025); 6	2025
8_Attachment 1	columns 8, 9 and 11	U.S.C. § 671 (3) ¹²	
	Asset Management,		
	column 11		

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 PREPA-of-LUMA-PROV-8_ROI-PREPA-LUMA-PROV-8_Attachment 1 under seal of confidentiality.

RESPECTFULLY SUBMITTED.

In San Juan, Puerto Rico, this 4th day of August 2025.

¹² These requests are consistent to those made requesting confidential treatment to portions of the Rate Review Petition submitted, mainly those related to IT, OT and Cybersecurity programs (see Request for Confidential Treatment of Portion of LUMA's Rate Review Petition (July 3, 2025) and the memorandum of law in support of such request (see Memorandum of Law in Support of Confidential Treatment of Portions of LUMA's Rate Review Petition (July 10, 2025)).

I 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, ifr@sbgblaw.com; Gabriela Castrodad, gcastrodad@sbgblaw.com; Jennise Alvarez, jennalvarez@sbgblaw.com; regulatory@genera-pr.com; José J. Díaz Alonso, jdiaz@sbgblaw.com; Stephen Romero Valle, sromero@sbgblaw.com; Giuliano Vilanovagvilanova@vvlawpr.com; Maraliz Vázquez-Marrero, mvazquez@vvlawpr.com; ratecase@genera-pr.com; regulatory@genera-pr.com; and legal@genera-pr.com; Co-counsel for Independiente Protección al Consumidor, hrivera@jrsp.pr.gov; **Oficina** de Instituto contratistas@jrsp.pr.gov; pvazquez.oipc@avlawpr.com; Co-counsel for Competitividad jpouroman@outlook.com; Sustentabilidad Económica, 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; jcunningham@whitecase.com; tmacwright@whitecase.com; mshepherd@whitecase.com; igreen@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; **PREPA** erickay@quinnemanuel.com; AdCo-Counsel for the Hoc 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 Energía nancy@emmanuelli.law; **Empleados** la Autoridad de Eléctrica. rafael.ortiz.mendoza@gmail.com; rolando@emmanuelli.law; monica@emmanuelli.law; cristian@emmanuelli.law; lgnq2021@gmail.com; Official Committee of Unsecured Creditors of PREPA, jcasillas@cstlawpr.com; jnieves@cstlawpr.com; Solar and Energy Storage Association Cfl@mcvpr.com; javrua@sesapr.org; of Puerto Rico. apc@mcvpr.com; mrios@arroyorioslaw.com; ccordero@arroyorioslaw.com; Wal-Mart Puerto Rico, Inc., Cfl@mcvpr.com; apc@mcvpr.com; Mr. Victor González, victorluisgonzalez@yahoo.com; and Bureau's Consultants, jrinconlopez@guidehouse.com; the Energy Josh.Llamas@fticonsulting.com; Anu.Sen@fticonsulting.com; Ellen.Smith@fticonsulting.com; rafael@maxetaenergy.com; Intisarul.Islam@weil.com; jorge@maxetaenergy.com; mcranston29@gmail.com; RSmithLA@aol.com; msdady@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. Notice will also be sent to

carl.pechman@keylogic.com; bernard.neenan@keylogic.com; tara.hamilton@ethree.com; aryeh.goldparker@ethree.com; roger@maxetaenergy.com; and Shadi@acciongroup.com.



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

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