COMMONWEALTH OF KENTUCKY
BEFORE THE PUBLIC SERVICE COMMISSION

In the Matter of:

ELECTRONIC APPLICATION OF NAVITAS KY NG, LLC FOR AN ALTERNATIVE FILING PURSUANT TO 807 KAR 5:076	**)** **)** **)**	**CASE NO. 2024-00252**

MOTION FOR CONFIDENTIAL TREATMENT

Navitas KY NG, LLC ("Navitas"), by counsel and pursuant to KRS § 61.878 and 807 KAR 5:001 Section 13, hereby moves the Kentucky Public Service Commission (the "Commission") to grant confidential protection to certain documents and information provided in connection with its Response to the Commission Staff's Second Request for Information in the above-styled matter (the "RFI"). The information for which Navitas seeks confidential treatment is hereinafter referred to as the "Confidential Information." In support of its Motion, Navitas states as follows:

1. Contemporaneously with the filing of this Motion, Navitas has filed its Response to the RFI and supporting exhibits in the above-referenced matter.

2. As discussed below, the Confidential Information is entitled to confidential treatment based upon KRS § 61.878(1)(a), KRS § 61.878(1)(c)(1), and KRS § 61.878(1)(m)(1).[1]

3. As part of its Response, Navitas has provided certain Confidential Information which is found throughout its Response to Request No. 2-10 and CONFIDENTIAL Exhibit PSC 2-10(d) attached thereto.

4. KRS § 61.878(1)(a) protects "records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal

[1] *See* 807 KAR 5:001, Section 13(2)(a)(1).

privacy." KRS § 61.878(1)(c)(1) protects "records confidentially disclosed to an agency or required by an agency to be disclosed to it, generally recognized as confidential or proprietary, which if openly disclosed would permit an unfair commercial advantage to competitors of the entity that disclosed the records." KRS § 61.878(1)(m)(1) protects certain "records the disclosure of which would have a reasonable likelihood of threatening the public safety by exposing a vulnerability in preventing, protecting against, mitigating, or responding to a terrorist act…." Subsection (f) of the previous cited statute explicitly includes infrastructure records that disclose "the location, configuration, or security of critical systems" and "critical systems" is defined therein to include "information technology" systems.

5. Request No. 2-10 seeks the following information: (i) identification of the specific billing software utilized by Navitas; (ii) how Navitas has configured said software; (iii) unique details regarding the installation of said software; and (iv) certain details regarding maintenance of said software. Navitas has identified risks associated with the public disclosure of this information that threaten the public safety as further explained herein.

I. Identification of the specific software used by Navitas will reduce the security and resilience of Navitas' information technology system. Due to the cost of customized software, small utilities, like Navitas, are forced to use "off the shelf" utility billing software products of which only a very small number exist. These products have open knowledge base articles, installation guides, and troubleshooting guides, so delineating publicly the specific software used by Navitas would assist a cybercriminal in maliciously accessing Navitas' information technology system.

II. Disclosure of how the software is configured will reduce the security and resilience of Navitas' information technology system. By delineating publicly if locally installed software is used, a cybercriminal can use that information to easily target the IP address of Navitas' local utility office for theft of credentials or a DDOS attack, which would effectively shut down operations. By delineating publicly if a remote/subscription service software is used, a cybercriminal can use that information to monitor inbound and outbound IP traffic from any of the Navitas' offices and spoof or intercept data required to gain access to the remote/subscription service software.

III. Release of the installation date of a particular brand of software will reduce the security and resilience of Navitas' information technology system. Delineating publicly the installation date of a particular software product would allow a cybercriminal to determine the approximate level of security/patches of the software utilized by Navitas and this would assist a cybercriminal in gaining malicious access to Navitas' information technology system.

IV. Release of information regarding the maintenance of the software will reduce the security and resilience of Navitas' information technology system. By delineating publicly if the software is not serviced by the manufacturer, a cybercriminal can use this information to assume Navitas is an easier target for malicious attacks like DDOS, Brute Force, and software specific issues based on the patch/installation date. By delineating publicly if the software is serviced by the manufacturer, a cybercriminal can use this information to conduct social engineering attacks on Navitas' employees to gain access which include

spoofing emails or calling Navitas' employees and pretending to be a support technician.

6. Simply put, public disclosure of the information requested in Response to PSC No. 2-10 materially increases the risk of a cybersecurity breach. A breach of Navitas' information technology system could result in cybercriminals accessing private information regarding Navitas' individual customers, including usage data, which would invade the customer's privacy rights. Navitas previously sought confidential treatment for customer-specific information similar to the type of information that could be exposed should Navitas' information technology system be compromised; this motion was granted by the Commission in an Order entered February 3, 2021 in which the Commission held that this information was "generally recognized as confidential or proprietary" and therefore met the criteria for confidential treatment.[2] The Commission has previously granted confidential treatment of such information pursuant to KRS § 61.878 for an indefinite period of time.[3]

7. In addition to public disclosure of information related to Navitas' information technology system increasing the risks of a cybersecurity breach, CONFIDENTIAL Exhibit PSC 2-10(d) contains Confidential Information which is not publicly disseminated and public disclosure of this information would harm Navitas. If potential competitors or other vendors enjoyed ongoing, unrestricted access to this Confidential Information, Navitas's ability to fairly

[2] *In the Matter of: Electronic Application of Navitas KY NG, Johnson County Gas Company, and B & H Gas System for Approval of Acquisition, Transfer of Ownership, and Control Of Natural Gas Utility Systems*, Case No. 2020-00396, Feb. 3, 2021 Order.

[3] *See In the Matter of: Application of Atmos Energy Corporation for an Adjustment of Rates and Tariff Modifications*, Case No. 2013-00148, Dec. 3, 2013 Order; *In the Matter of: Filing of Agreement for the Purchase and Sale of Firm Capacity and Energy Between Big Rivers Electric Corporation and the Kentucky Municipal Energy Agency*, Order, P.S.C. Case No. 2016-00306 (Jan. 2, 2019); *In the Matter of: Application of Kentucky Utilities Company for an Adjustment of its Electric Rates*, Order, P.S.C. Case No. 2012-00221 (July 25, 2013) (holding customer names, account numbers, and usage information exempt from disclosure under KRS § 61.878(1)(a)).

negotiate terms with counterparties in the marketplace would be negatively impacted. Indeed, the public disclosure of this Confidential Information will inevitably inure to the benefit of Navitas's potential counterparties and competitors, which would gain valuable, non-public information about Navitas's business. Information such as this is generally recognized as confidential or proprietary.[4]

8. By keeping the information sought in Request No. 2-10, including the Exhibits provided therewith, confidential, the risks identified in Section 5 of this Motion would be avoided which prevents a decrease in the overall security of Navitas' information technology system and ensures the continuing security of Navitas' information technology system.

9. Navitas seeks confidential treatment for the entirety of its Response to Request No. 2-10, including Exhibits thereto. As identified herein, that Response includes information regarding the configuration and security of its information technology system which is a critical system.[5] Further, revealing this information could endanger Navitas' customer's personal information.[6] And finally this response contains information that could provide an unfair commercial advantage to competitors or counterparties of Navitas, as it contains sensitive cost data the public disclosure of which could disadvantage Navitas in future negotiations for similar

[4] *See, e.g.*, Case No. 2021-00278, *Electronic Purchased Gas Adjustment Filing of Navitas KY NG, LLC*, Order (Ky. PSC Aug. 16, 2022); *Hoy v. Kentucky Indus. Revitalization Authority*, 907 S.W.2d 766, 768 (Ky. 1995) ("It does not take a degree in finance to recognize that such information concerning the inner workings of a corporation is 'generally recognized as confidential or proprietary'"); *Marina Management Servs. v. Cabinet for Tourism, Dep't of Parks*, 906 S.W.2d 318, 319 (Ky. 1995) (unfair commercial advantage arises simply from "the ability to ascertain the economic status of the entities without the hurdles systemically associated with the acquisition of such information about privately owned organizations"); Case No. 2019-00115, *In the Matter of: Electronic Application of Grayson County Water District for a Deviation from Meter Testing Requirements of 807 KAR 5:066, Section 16(1)*, Order (Ky. P.S.C. September 19, 2019) (granting confidential protection for proprietary product produced by a third party that was not available to the general public/required membership to obtain and was generally recognized as confidential).

[5] *See* KRS § 61.878(1)(m)(1).

[6] *See* KRS § 61.878(1)(a).

services.[7] Navitas respectfully asks that the Commission treat the entirety of Response to Request 2-10 confidentially in accordance with KRS § 61.878(1)(m)(1).

10. Consistent with the above discussion, Navitas respectfully requests the Commission enter an order granting confidential treatment to the Response to Request 2-10, including the Exhibit thereto.

11. This Confidential Information is not publicly available, is not disseminated within Navitas except to those employees and professionals with a legitimate business need to know and act upon the information, and is not disseminated to others without a legitimate need to know and act upon the information.

12. Navitas requests indefinite protection for the information technology system information identified in Response to Request 2-10 and CONFIDENTIAL Exhibit PSC 2-10(d). Ensuring the continued protection of this information promotes security for Navitas' information technology system and the public for as long as the information remains relevant/accurate, and thus the information should remain confidential indefinitely.

13. If and to the extent the Confidential Information becomes generally available to the public, whether through filings required by other agencies or otherwise, Navitas will notify the Commission in writing.[8]

14. If the Commission disagrees with Navitas that the material for which this Motion seeks confidential treatment is exempt from disclosure, it must hold an evidentiary hearing to protect the due process rights of Navitas and permit the opportunity to supply the Commission with a complete record to enable it to reach a decision with regard to this confidentiality request.

[7] *See* KRS § 61.878(1)(c)(1).
[8] 807 KAR 5:001 Section 13(10)(b).

15. In compliance with 807 KAR Section 8(3) and Section 13(2)(e), Navitas is filing with the Commission a copy of the Confidential Information, unredacted and with the confidential information highlighted or similarly indicated. The unredacted copies are filed under seal pursuant to the instructions regarding confidential filings in the March 24, 2020 Order issued in Case No. 2020-00085; redacted pages of the subject documents (or appropriate placeholders, in the case confidentiality is sought for the entirety of a document) are being publicly filed.

WHEREFORE, Navitas respectfully requests that the Commission classify and protect as confidential the Confidential Information.

This 22nd day of November, 2024.

Respectfully submitted,

DINSMORE & SHOHL LLP

/s/ M. Evan Buckley

M. Evan Buckley
Alexander H. Gardner
100 West Main Street, Suite 900
Lexington, Kentucky 40507
E-mail: evan.buckley@dinsmore.com
E-mail: alexander.gardner@dinsmore.com
Phone: (859) 425-1000
Fax: (859) 425-1099

R. Brooks Herrick
101 South 5th Street, Suite 2500
Louisville, KY 40202
E-mail: brooks.herrick@dinsmore.com
Telephone: (502) 540-2300
Facsimile: (502) 585-2207

Counsel to Navitas KY NG, LLC

Certification

I hereby certify that a copy of the foregoing has been served electronically on all parties of record through the use of the Commission's electronic filing system, and there are currently no parties that the Commission has excused from participation by electronic means. Pursuant to the Commission's July 22, 2021 Order in Case No. 2020-00085, a paper copy of this filing has not been transmitted to the Commission.

/s/ M. Evan Buckley
Counsel to Navitas KY NG, LLC