APPENDIX C9

CYBERSECURITY REQUIREMENTS

1. Cyber Security, General Security Requirements.

   a. Defined Terms. For purposes of this appendix, the following terms shall have the following meanings:

      "CHGE Information" means all information, data, compilations, studies, documents, telemetry, and metadata relating to the Project to which Central Hudson Gas and Electric Corporation ("CHGE") is entitled, whether exchanged pursuant to Exhibit H (Communication Protocols) in the Energy Storage Services Agreement ("ESSA"), or otherwise pursuant to the terms of the ESSA, or any other agreement to which CHGE and Owner are parties.

      "Services" means those services provided pursuant to the ESSA.

      "Process" "Processing" and "Processed" mean any action or operation that is performed using or upon CHGE Information whether it be by physical, automated or electronic means, including without limitation, the use, access, storage, transfer, hosting, collection, recording, organization, maintenance, handling, retrieval, disclosure, sharing, dissemination, copying, processing, erasure, deletion, or destruction.

      "Owner Personnel" means Owner, Owner's Affiliates and their respective officers, directors, employees, agents and subcontractors.

   b. Interpretation. For purposes of this appendix, Owner shall cause the applicable Owner Personnel to comply with, and shall be responsible for any breach of, any obligation of Owner Personnel hereunder.

   c. If Owner Personnel connect to the computing systems or networks of CHGE, Owner agrees, that: (i) Owner Personnel will not access, and will not permit any other person or entity to access, CHGE's computing systems or networks without CHGE's authorization and any such actual or attempted access shall be consistent with any such authorization; (ii) all Owner Personnel connectivity to CHGE's computing systems and networks and all attempts at same shall be only through CHGE's security gateways/firewalls; and (iii) Owner Personnel shall use industry standard virus and malware detection/scanning program prior to any attempt to access CHGE's computing systems or networks.

   d. To the extent required by CHGE based on the type of work being performed by Owner Personnel or the type of access being granted to Owner Personnel to CHGE facilities, systems, or infrastructure, Owner shall, in accordance with all applicable Laws, perform background investigations of Owner Personnel performing work under this Agreement which requires such background investigation, and shall supply CHGE with evidence, as requested, that such background checks have been performed and have returned "clear" or

otherwise satisfactory results. Owner shall not allow any Owner Personnel to perform services under this Agreement prior to obtaining "clear" or otherwise satisfactory background check results.

e. Without limiting the foregoing provisions, if CHGE gives Owner Personnel access (either on-site or remotely) to the networks or computer systems of CHGE, Owner Personnel shall limit its authorized access and use to those computer systems, files, software, or services reasonably required to perform the Services.

f. Owner represents that all information provided to CHGE in connection with CHGE's information technology security assessment evaluation of Owner Personnel and any applicable software (including, without limitation, Owner Personnel responses to CHGE's Owner Product/Service Security Assessment Checklist) is true, accurate and complete in all material respects and if there is a change in such information or such information becomes or is discovered to be untrue, then Owner shall notify CHGE as soon as practically possible. Owner Personnel shall cooperate with all reasonable information technology security procedures and requirements as may be issued to Owner by CHGE from time to time during the Term.

g. Owner Personnel shall comply with any additional access, safety and security requirements and procedures (including cybersecurity requirements and procedures) which CHGE provides to Owner in writing.

2. Information Security Matters.

a. Information Security Program.

i. Owner Personnel shall:

1. develop, implement, maintain, and monitor a comprehensive, written information security program that contains administrative, technical, and physical safeguards to protect against anticipated threats or hazards to the security, confidentiality or integrity of, the unauthorized or accidental destruction, loss, alteration or use of, and the unauthorized access to, acquisition of or Processing of CHGE Information ("Information Security Program"); and

2. conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of electronic, paper, and other records containing CHGE Information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks.

ii. Owner Personnel shall review and, as appropriate, revise its Information Security Program: (i) at least annually or whenever there is a material change in Owner or its Affiliates' business practices that may reasonably affect the security or integrity of CHGE Information; (ii) whenever there is a change in Exhibit H (Communication Protocols); (iii) in accordance with prevailing industry practices and Applicable Law;

and (iv) as reasonably requested by CHGE. If Owner Personnel modifies its Information Security Program following such a review, Owner shall promptly notify CHGE of the modifications and shall provide the modifications to CHGE in writing upon CHGE's request. Owner Personnel may not alter or modify its Information Security Program in such a way that will weaken or compromise the confidentiality, security and integrity of CHGE Information.

iii. Owner Personnel shall maintain and enforce its Information Security Program at each location from which Owner provides the Services.

iv. Owner Personnel shall ensure that its Information Security Program covers all networks, systems, servers, computers, notebooks, laptops, mobile phones, and other devices and media that Processes CHGE Information or that provides access to CHGE networks, systems or information.

v. Owner Personnel shall ensure that its Information Security Program includes industry standard password protections, firewalls and anti-virus and malware protections to protect CHGE Information stored on computer systems.

vi. Owner Personnel shall conduct security testing at least once per calendar year using a third party to provide monitoring, penetration and intrusion testing with respect to Owner Personnel's systems at and promptly provide a copy of the results to CHGE, provided that Owner may redact IP addresses and other client names and information. To the extent any issues are identified in such testing, Owner shall take commercially reasonable efforts to address such issues as recommended by such third-party provider and shall promptly notify CHGE of the steps taken by Owner.

b. Data Access Controls. Owner agrees that: (i) Owner Personnel shall maintain appropriate access controls, including, but not limited to, limiting access to CHGE Information to the minimum number of Owner Personnel who require such access in order to provide Services to CHGE under this Agreement and (ii) Owner Personnel who will be provided access to, or otherwise come into contact with, CHGE Information will be required (including during the term of their employment or retention and thereafter) to protect such CHGE Information in accordance with this Section 2, and will have entered into appropriate confidentiality agreements or be bound by appropriate obligations of confidentiality.

****** End of APPENDIX ******