ADDENDUM TO PURCHASE ORDER FOR PRODUCTS AND SERVICES ASSOCIATED WITH NERC CIP HIGH AND MEDIUM IMPACT BULK ELECTRIC SYSTEM ("BES") CYBER SYSTEMS AND THEIR ASSOCIATED EACMS AND PACS: CIP-013 RELIABILITY STANDARD REQUIREMENTS

This Addendum to Purchase Order for Products and Services Associated with NERC CIP High and Medium Impact Bulk Electric System ("BES") Cyber Systems and their associated EACMS and PACS, defined below, ("NERC CIP-013 Addendum") is made part of and incorporated into the Purchase Order by and between the Contractor and Company (as defined below). The terms of this Addendum shall take precedence over any conflicting or inconsistent terms of the Purchase Order. Non-conflicting terms in the Purchase Order shall continue to apply. In addition, defined terms used herein shall have the meanings set forth below or the meaning ascribed to them in the Purchase Order.

1. Definitions

The following definitions apply only to the terms and conditions in this Addendum:

"**CIP**" means Critical Infrastructure Protection Electric Reliability Standards adopted and enforced by NERC.

"Company" means Long Island Electric Utility Servco LLC ("Agent"), as agent of and acting on behalf of the Long Island Lighting Company d/b/a LIPA ("LIPA" or "Company) that acquires or procures a product or service for the purchase or acquisition of BES or other Materials that are covered by the NERC CIP-013 reliability standard requirements.

"Company Data" means for purposes of this NERC CIP-013 Addendum, any and all information concerning Company or Agent and their business in any form, including, without limitation, the products and services provided under this Contract that is Disclosed to or otherwise learned by Contractor during the performance of this Contract.

"Contractor" means the organization or individual that enters into an agreement with Company for supplying a product or service. For clarification and purposes of this NERC CIP-013 Addendum, "Consultant", "Supplier" "Seller" or "Vendor", or other term used to identify the organization or individual described herein, shall have the same meaning.

"Contract" or "Contract Documents" means the documents that make up the entire agreement between Company and Contractor with respect to the product or service supplied including this NERC CIP-013 Addendum. Contract or Contract Documents may also be used interchangeably with, and have the same meaning as Purchase Order.

"Cyber Assets" means programmable electronic devices, including the hardware, software, and data in those devices.

"Disclosed" means any circumstance when the security, integrity, or confidentiality of any Company Information has been compromised, including but not limited to incidents where

Company Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for an unauthorized purpose.

"EACMS" means Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.

"Electronic Security Perimeter" means the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.

"Interactive Remote Access" means user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol. Remote access originates from a Cyber Asset that is not an Intermediate System and not located within any of Company's Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by Company, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.

"Intermediate Systems" means a Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users. The Intermediate System must not be located inside the Electronic Security Perimeter.

"**NERC**" means the North American Electric Reliability Corporation in its role as the Federal Energy Regulatory Commission's certified electric reliability organization.

"PACS" means Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers.

"Physical Security Perimeter" means the physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled.

"**PII"** means Personally Identifiable Information.

"Security Incident" means any circumstance when (i) Contractor knows or reasonably believes that Company Information hosted or stored by the Contractor has been Disclosed; (ii) Contractor knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided to Company by Contractor or the physical, technical, administrative, or organizational safeguards protecting Contractor's systems or Company's systems storing or hosting Company Information; or (iii) Contractor receives any complaint, notice, or communication which relates directly or indirectly to a Security Incident involving (A) Contractor's handling of Company Information or Contractor's compliance with the data

safeguards in this Purchase Order or applicable laws in connection with Company Information or (B) the cybersecurity of the products and services provided to Company by Contractor.

2. Notification by Contractor

Contractor agrees to notify Company's IT Security, immediately (but in no case later than twenty-four (24) hours) after becoming aware of any Security Incident by e-mail at ITSecurity@pseg.com whenever a Security Incident occurs.

The notice shall include the date and time of the Security Incident's occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of (a) why the Security Incident occurred (e.g., a description of the reason for the system failure), (b) the amount of Company Information known or reasonably believed to have been Disclosed, and (c) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

Contractor shall provide written updates of the notice to Company addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances.

Contractor shall reasonably cooperate with Company in Company's efforts to determine the risk posed by the Security Incident, including providing additional information regarding the Security Incident upon request from Company.

3. Development and Implementation of a Response Plan

Contractor shall develop and implement a "Response Plan," that shall include policies and procedures to address Security Incidents. The Response Plan shall include appropriate provisions for mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence(s) to prevent the recurrence of similar Security Incidents in the future. The Response Plan shall include appropriate provisions for mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence to prevent the recurrence of Security Incidents in the future. Contractor shall provide Company access to inspect its Response Plan. The development and implementation of the Response Plan shall follow industry standard practices, such as those that at a minimum are consistent with the contingency planning requirements of National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide, Special Publication 800-61 Rev. 2 and NIST Computer Security Incident Handling Guide, Special Publication 800-61 Rev. 2 (2012), NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 (NIST, Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800-53 Rev. 4 (2012), note CP-1 through CP-13 cover Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing, Contingency Plan Update, Alternate Storage Site, Alternate Processing Site, Telecommunications Services, Information System Backup, Information System Recovery and Reconstitution, Alternate Communications Protocols, Safe Mode, and Alternative Security Mechanisms) and the incident response

requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended.

Immediately upon learning of a Security Incident related to the products and services provided to Company, Contractor shall implement its Response Plan and, within 24 hours of implementing its Response Plan, shall notify Company in writing of that implementation as described above.

Prevention of Recurrence: Within 30 days of a Security Incident, Contractor shall develop and execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and industry standards (e.g., NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, as may be amended (NIST Special Publication 800-61 (Rev. 2) (2012) and NIST Guide for Cybersecurity Event Recovery, Special Publication 800-184 (2016)) and shall communicate that plan to Company. Contractor shall provide recommendations to Company on actions that Company may take to assist in the prevention of recurrence, as applicable or appropriate. Company may take such actions in its sole discretion but shall not be obligated to take any such actions.

Coordination of Incident Response with Company: Within two (2) Business Days of notifying Company in writing of the Security Incident, Contractor shall recommend actions to be taken by Company on Company-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls and the location(s), if applicable, where response is required. Contractor shall coordinate with Company in developing those action plans and mitigating controls. Contractor will provide Company guidance, recommendations and other necessary information for recovery efforts and long term remediation and/or mitigation of cyber security risks posed to Company Information, equipment, systems, and networks as well as any information necessary to assist Company in relation to the Security Incident.

Notification to Affected Parties:

(a) Contractor will, at its sole cost and expense, assist and cooperate with Company with respect to any investigation of a Security Incident, disclosures to affected parties, and other remedial measures as requested by Company in connection with a Security Incident or required under any applicable laws related to a Security Incident.

(b) In the event a Security Incident results in Company Information being Disclosed, such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of Company under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by Company, except as required by applicable law or approved by Company in writing. Company will have sole control over the timing and method of providing such notification.

Unrelated Security Incidents: In the event:

(a) Contractor Proprietary Information, related to the products and/or services provided to the Company under this Contract, has been corrupted or destroyed or has been accessed, acquired, compromised, modified, used or Disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose;
(b) Contractor knows or reasonably believes that an act or omission has compromised the cybersecurity of the products and services provided by Contractor to an entity other than Company; or
(c) Contractor receives any valid complaint, notice, or communication that relates directly or indirectly to (i) Contractor's handling of Contractor Proprietary Information or Contractor's compliance with applicable law in connection with Contractor Proprietary Information or (ii) the cybersecurity of the products and services provided by Contractor to an entity other than Company ("Unrelated Security Incident"),

Contractor shall provide to Company a confidential report describing, to the extent legally permissible, a detailed summary of the facts and circumstances of the Unrelated Security Incident, including a description of (a) why the Unrelated Security Incident occurred, (b) the nature of the Contractor Proprietary Information disclosed, and (c) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

4. Development and Implementation of Access Control Policy

Contractor shall develop and implement policies and procedures to address the security of Contractor's remote and onsite access to Company Information, Company systems and networks, and Company property ("Access Control Policy") that is consistent with the personnel management requirements of industry standard practices (e.g. NIST Special Publication 800-53 Rev. 4 AC-2 (covers account management), PE-2 (covers physical access authorization), PS-4(covers personnel termination), and PS-5(covers personnel transfer), as may be amended, and also meets the following requirements:

Company Authority Over Access: In the course of furnishing products and services to Company under this Agreement, Contractor shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Contractor Personnel") to access Company's property, systems, or networks or Company Information without Company's prior express written authorization. Such written authorization may subsequently be revoked by Company at any time in its sole discretion. Further, any Contractor Personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Company. All Company authorized connectivity or attempted connectivity to Company's systems or networks shall be in conformity with Company's security policies, as may be amended from time to time with notice to the Contractor.

Contractor Review of Access: Contractor will review and verify Contractor Personnel's continued need for access and level of access to Company Information and Company systems, networks and property on a quarterly basis and will retain evidence of the reviews for two years from the date of each review.

Notification and Revocation: Contractor will notify Company within 12 hour(s) in writing (no later than close of business on the same day as the day of termination or change set forth below):

(i) any Contractor Personnel no longer requires such access in order to furnish the services or products provided by Contractor under this Contract ,

(ii) any Contractor Personnel is terminated or suspended or his or her employment is otherwise ended,

(iii) Contractor reasonably believes any Contractor Personnel poses a threat to the safe working environment at or to any Company property, including to employees, customers, buildings, assets, systems, networks, trade secrets,
confidential data, and/or Company Information,

(iv) there are any material adverse changes to any Contractor Personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record,

(v) any Contractor Personnel loses his or her U.S. work authorization, or,

(vi) Contractor's provision of products and services to Company under this Contract is either completed or terminated, so that Company can discontinue electronic and/or physical access for such Contractor Personnel.

Contractor will take all steps reasonably necessary to immediately revoke such Contractor Personnel electronic and physical access to Company Information as well as Company property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multifactor security tokens, and laptops, as applicable. Further, for such revoked Contractor Personnel, Contractor will return to Company any Company-issued property including, but not limited to, Company photo ID badge, keys, parking passes, documents, or electronic equipment in the possession of such Contractor Personnel. Contractor will notify Company at PSEG.contractor.termination.notice@pseg.com once access to Company Information as well as Company property, systems, and networks has been removed.

5. Disclosure and Remediation of Vulnerabilities

Contractor shall, at its sole cost and expense, develop and implement policies and procedures to address the disclosure and remediation by Contractor of vulnerabilities and material defects related to the products and services provided to Company under this Contract including the following:

(a) Prior to the delivery of the procured product or service, Contractor shall provide or direct Company to an available source of summary documentation of publicly disclosed vulnerabilities and material defects related in the procured product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

(b) Contractor shall provide or direct Company to an available source of summary documentation of vulnerabilities and material defects in the procured product or services within thirty (30) calendar days after such vulnerabilities and material defects become known to Contractor. The summary documentation shall include a description of each vulnerability and material defects and its potential impact, root cause, and recommended

corrective actions, compensating security controls, mitigations, and/or procedural workarounds (e.g., monitoring).

(c) Contractor shall disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written attestation that all such backdoors created by Contractor have been permanently remediated.

(d) Contractor shall implement a vulnerability detection and remediation program consistent with industry standards (e.g., ISO-29147 Vulnerability Disclosure, NIST Cybersecurity Framework v1.1 Reference RS.AN-5, NIST Special Publication 800-53 Rev. 4 RA-5, vulnerability detection and remediation program consistent with NIST Special Publication 800-53 Rev. 4 RA-5, SA-11, 19 and SI-2, as may be amended.2018 SA-11, and SI-2, as may be amended).

Disclosure of Vulnerabilities by Company: Whether or not publicly disclosed by Contractor and notwithstanding any other limitation in this Contract, Company may disclose any vulnerabilities, material defects and/or other findings related to the products and services provided by Contractor to (a) the Electricity Information Sharing and Analysis Center ("E-ISAC"), the United States Cyber Emergency Response Team ("CERT"), or any equivalent U.S. governmental entity or program, (b) to any applicable U.S. governmental entity when necessary to preserve the reliability of the BES as determined by Company in its sole discretion, or (c) any entity required by applicable law.

6. Hardware, Firmware, Software, and Patch Integrity and Authenticity

(a) Contractor shall establish, document, and implement risk management practices for supply chain delivery of software (including patches), and firmware provided under this Contract. Contractor shall provide documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on how to request replacement parts, and commitments to ensure that spare parts shall be made available by Contractor as determined by Company in its sole discretion.

(b) Contractor shall specify how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If Company deems that it is warranted, Contractor shall apply encryption technology to protect procured products throughout the delivery process.

(c) If Contractor provides software or patches to Company, Contractor shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable Company to use the hash value as a checksum to independently verify the integrity of the software and patches. .

(d) Contractor shall identify or provide Company with a method to identify the country (or countries) of origin of the procured Contractor product and its components (including hardware, software, and firmware). Contractor will identify the countries where the development, manufacturing, maintenance, and service for the Contractor product are provided. Contractor will notify Company of changes in the list of countries where product maintenance or other services are provided in support of the procured Contractor product.

This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.

(e) Contractor shall provide a software bill of materials for procured (including licensed) products consisting of a list of components and associated metadata that make up a component.

(f) Contractor shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

(g) Contractor shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

(h) Contractor shall demonstrate chain-of-custody documentation for procured products as determined by Company in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

Patching Governance:

(a) Prior to the delivery of any products and services to Company or any connection of electronic devices, assets, or equipment to Company's electronic equipment, Contractor shall provide documentation regarding its patch management and vulnerability, management/mitigation programs and update process (including third-party, software, and firmware) for products, services, and any electronic device, asset, or equipment required by Contractor to be connected to the assets of Company during the provision of products and services under this Contract. This documentation shall include information regarding:

(i) the resources and technical capabilities to sustain this program and process such as the method or recommendation for how the integrity of a patch is validated by Company; and

(ii) the approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

b) Unless otherwise approved by the Company in writing, the current or supported version of Contractor products and services supplied by Contractor shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components (e.g., Java, Flash, Web browser, etc.).

(c) Contractor shall verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to Company.

(d) In providing the products and services described in this Contract, Contractor shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for Contractor products within thirty (30) days. Updates to remediate critical vulnerabilities shall be provided within twenty-one (21) days. If updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations, methods of exploit detection and/or work-arounds within thirty (30) days.

(e) When third party hardware, software (including open-source software), and firmware is provided by Contractor to Company, Contractor shall provide appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses if applicable to the Company's use of the third-party product in its system environment, within thirty (30) days of availability from the original supplier and/or

patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment shall be provided within a shorter period than other updated, within sixty (60) days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, Contractor shall provide or arrange for the provision of recommended mitigations, and/or workarounds within thirty (30) days

Viruses, Firmware and Malware:

(a) Contractor will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to Company. To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable effort to ensure the third-party investigates whether computer viruses or malware are present in any software or patches provided to Company or being installed on Company's information networks, computer systems, and information systems.

(b) Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality. To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable efforts to ensure the third-party will not insert any code that would have the effect of disabling or otherwise shutting down all, or a portion of, such software or damaging information or functionality.

(c) When installed files, scripts, firmware, or other Contractor-delivered software solutions (including third-party installed files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor, Contractor must provide technical justification as to why the "false positive" hit has taken place to ensure its code's supply chain has not been compromised.

(d) If a virus or other malware is found to have been coded or otherwise introduced as a direct result of Contractor's breach of its obligations under this Contract, Contractor shall upon written request by Company and at its own cost:

(i) Take all necessary remedial action and provide assistance to Company to eliminate the virus or other malware throughout Company's information networks, computer systems, and information systems, and

(ii) If the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Contractor is obligated under this Contract to back up such data, take all steps necessary and provide all assistance required by Company and its affiliates, or (B) where Contractor is not obligated under this Contract to back up such data, use commercially reasonable efforts in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

End of Life Operating Systems:

(a) Contractor delivered solutions will not be required to reside on end-of-life operating systems, or any operating system that will go end-of-life six (6) months from the date of installation.

(b) Contractor solutions will support the latest versions of operating systems on which Contractor-provided software functions within twenty-four (24) months from official public release of that operating system version.

Cryptographic Requirements:

(a) Contractor shall document how the cryptographic system supporting the Contractor's products and/or services procured under this Contract protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to, the following:

(i) The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm [SHA]-256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.

(ii) The preoperational and operational phases of key establishment, deployment, on-going validation, and revocation.

(b) Contractor will use only "approved" cryptographic methods as defined in the FIPS 140-2 Standard when enabling encryption on its products.

(c) Contractor shall provide or arrange for the provision of an automated remote key establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

(d) Contractor shall ensure that:

(i) The system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, as may be amended.

(ii) The key update method supports remote re-keying of all devices within 30 days as part of normal system operations.

(iii) Emergency re-keying of all devices can be remotely performed within 30 days.

(e) Contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

7. Coordination of Controls

Contractor shall coordinate with Company on all remote access to Company's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by Company.

Controls for Remote Access: Contractors that directly, or through any of their affiliates, subcontractors or service providers, connect to Company's systems or networks agree to the additional following protective measures:

(a) Contractor will not access, and will not permit any other person or entity to access, Company's systems or networks without Company's written authorization and any such actual or attempted access will be consistent with any such written authorization.

(b) Contractor shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.

(c) Contractor shall ensure Contractor Personnel do not use any virtual private network or other device to simultaneously connect machines on any Company system or network to any machines on any Contractor or third-party systems, without

(i) using only a remote access method consistent with Company's remote access control policies, (providing Company with the full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and

(iii) ensuring that any computer used by Contractor Personnel to remotely access any Company system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Company systems or networks.

(d) Contractor shall ensure Contractor Personnel accessing Company networks are uniquely identified and that accounts are not shared between Contractor Personnel.