CONSOLIDATED EDISON COMPANY OF NEW YORK, INC.

SPECIAL CONDITIONS

FOR

MANAGING SUPPLY CHAIN AND CYBER SECURITY RISKS

May 23, 2022

TABLE OF CONTENTS

Page

Nature of These Special Conditions

These Special Conditions for Managing Supply Chain and Cyber Security Risks[1] ("Special Conditions") have been developed as part of Con Edison's Supply Chain cyber security risk management plan, which is intended to: (i) address North American Electric Reliability Corporation ("NERC") Reliability Standard CIP-013-1, which Reliability Standard supplements the NERC Critical Infrastructure Protection ("CIP") Standards, (ii) mitigate cyber security risks associated with the supply chain and address related information and data protection, and (iii) require vendor cooperation in the protection of the security of the supply chain. Section headings that are underlined and in bold font and Requirement numbers (e.g., R1.2.1) are from NERC Reliability Standard CIP-013-1 and are for reference purposes only.

These Special Conditions may be used in conjunction with other Con Edison Standard Terms and Conditions, such as the Con Edison Standard Terms and Conditions for Professional Services Contracts, Con Edison Standard Terms and Conditions for Purchase of Equipment, or Con Edison Standard Terms and Conditions for Service Contracts. If there is a conflict between these Special Conditions and any other terms and conditions contained in the Contract: (i) and if there is a typewritten provision of the BPA, CPA, purchase order form or other special conditions incorporated by reference therein that expressly refers by number and title to the conflicting provision in these Special Conditions and states that such provision does not apply, then in such case the conflicting typewritten provision of the BPA, CPA, purchase order form or other special conditions incorporated by reference therein shall take precedence and govern, (ii) and if there is no such typewritten provision, then in such case the provision that is more protective of Con Edison, Con Edison Information, and the goods and services provided to Con Edison under the Contract and more effectively mitigates the risks associated with the supply chain shall take precedence and govern.

Definitions

The following definitions apply only to the terms and conditions in these Special Conditions:

"Bulk Electric System" ("BES") shall have the meaning ascribed to it in the NERC Reliability Standards, as updated.

"**Business Day**" means Monday through Friday, except for Con Edison designated holidays.

"**Con Edison**" means Consolidated Edison Company of New York, Inc., the entity entering into the Contract and issuing any purchase orders applicable to the Contract, for goods or services to be furnished to Con Edison or its affiliates, Orange and Rockland Utilities, Inc. ("O&R") and Con Edison Transmission, Inc. ("CET"). For the avoidance of doubt, "goods" shall include but not be limited to equipment, hardware, products, and digital products such as software programs, applications, firmware, computer code, data and information.

"**Con Edison Information**" means for purposes of these Special Conditions, any and all information concerning Con Edison and its business in any form, including, without limitation, the goods and services provided under the Contract, that is disclosed to or otherwise learned by Supplier during the performance of the Contract.

"**Contract**" means the contract between Con Edison and Supplier consisting of (a) a Blanket Purchase Agreement ("BPA"), Contract Purchase Agreement ("CPA") and/or Standard Purchase

[1] These Special Conditions are based on the "Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk", © 2019 by the Edison Electric Institute (EEI).

Order ("purchase order"), (b) the relevant Con Edison request for quotation, (c) these Special Conditions, and (d) any documents or portions thereof incorporated by reference in (a), (b), or (c) above, including, but not limited to, other special conditions, specifications, performance requirements, plans, schedules and drawings.

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

"**Security Incident**" means any circumstance when (i) Supplier knows or reasonably believes that Con Edison Information hosted or stored by the Supplier has been Disclosed; (ii) Supplier knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cyber security of the goods or services provided to Con Edison by Supplier or the physical, technical, administrative, or organizational safeguards protecting Supplier's systems or Con Edison's systems storing or hosting Con Edison Information; or (iii) Supplier receives any complaint, notice, or communication which relates directly or indirectly to a Security Incident involving (A) Supplier's handling of Con Edison Information or Supplier's compliance with the data safeguards in the Contract or applicable laws in connection with Con Edison Information or (B) the cyber security of the goods or services provided to Con Edison by Supplier.

"**Supplier**" means the seller or contractor, as the case may be, who is a party to the Contract with Con Edison.

"**Supplier Personnel**" shall have the meaning set forth in Section 3(b) below.

"**Virus**" means any computer code designed to allow unauthorized access to or to disable, delete, disrupt or damage Con Edison's use of the goods or services furnished under the Contract, any Con Edison computer, system or network, or any data residing on any Con Edison computer, system or network, without Con Edison's express written consent including, without limitation, viruses, malware, ransomware, adware, worms, time bombs, Trojan horses, or other harmful, malicious or destructive computer code.

1. <u>Notification by the Vendor of Vendor-Identified Incidents Related to the Products or Services Provided to the Responsible Entity That Pose Cyber Security Risk to the Responsible Entity (Requirement R1.2.1)</u>

(a) Supplier agrees to notify the Con Edison authorized representative, by telephone and e-mail, of a Security Incident before the end of the next Business Day following the occurrence of the Security Incident.

(b) The written notice shall include the date and time of the Security Incident 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 Con Edison 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.

(c) Supplier shall provide written updates of the notice to Con Edison 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.

(d) Supplier shall cooperate with Con Edison in Con Edison's efforts to determine the risk posed by the Security Incident, including providing additional information regarding the Security Incident upon request from Con Edison.

2. <u>Coordination of Responses to Vendor-Identified Incidents Related to the Products or Services Provided to the Responsible Entity That Pose Cyber Security Risk to the Responsible Entity (Requirement R1.2.2)</u>

(a) Development and Implementation of a Response Plan: Supplier shall develop and implement a "Response Plan" which 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. Supplier shall provide Con Edison access to inspect its Response Plan. At a minimum, 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 NIST Special Publication 800-61 Rev. 2, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended. Without limiting the foregoing, the Response Plan shall include the following:

- One or more processes to identify and respond to Security Incidents
- The roles and responsibilities of Security Incident response groups or individuals
- Incident handling procedures for Security Incidents
- Procedures for reducing the likelihood of the same or a similar Security Incident from occurring in the future

Immediately upon learning of a Security Incident related to the goods and services provided to Con Edison, Supplier shall implement its Response Plan and, by close of business of the next Business Day following the implementation of the Response Plan, notify Con Edison in writing of that implementation by contacting the Con Edison authorized representative.

(b) Prevention of Recurrence: Within 60 days of a Security Incident, Supplier 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) and shall communicate that plan to Con Edison. Supplier shall provide recommendations to Con Edison on actions that Con Edison may

take to assist in the prevention of recurrence, as applicable or appropriate.

(c) Coordination of Incident Response with Con Edison: Within 30 days of notifying Con Edison in writing of the Security Incident, Supplier shall recommend actions to be taken by Con Edison on Con Edison-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. Supplier shall coordinate with Con Edison in developing those action plans and mitigating controls. Supplier will provide Con Edison guidance, recommendations and other necessary information for recovery efforts and long term remediation and/or mitigation of any cyber security risks posed to Con Edison Information, equipment, systems, and networks as well as any information necessary to assist Con Edison in relation to the Security Incident.

(d) Notification to Affected Parties:

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

ii. In the event a Security Incident results in Con Edison 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 Con Edison 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 Con Edison, except as required by applicable law or approved by Con Edison in writing. Con Edison will have sole control over the timing and method of providing such notification.

3. <u>Notification by Vendors When Remote or Onsite Access Should No Longer be Granted to Vendor Representatives (Requirement R1.2.3)</u>

(a) Development and Implementation of Access Control Policy: Supplier shall develop and implement policies and procedures to address the security of Supplier's remote and onsite access to Con Edison Information, Con Edison systems and networks, and Con Edison property (an "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, PE-2, PS-4, and PS-5 as may be amended) and also meets the requirements set forth in Sections 3(b) – 3(d) below.

(b) Con Edison Authority Over Access: In the course of furnishing goods and services to Con Edison under the Contract, Supplier shall not access, and shall not permit its employees, agents, contractors, and other personnel or entities within its control ("Supplier Personnel") to access Con Edison's property, systems, or networks or Con Edison Information without Con Edison's prior express written authorization. Such written authorization may subsequently be revoked by Con Edison at any time in its sole discretion.

Further, any Supplier Personnel access shall be consistent with, and in no case exceed the scope of, any such approval granted by Con Edison. All Con Edison authorized connectivity or attempted connectivity to Con Edison's systems or networks shall be in conformity with Con Edison's security policies as may be amended from time to time with notice to the Supplier.

(c) Supplier Review of Access: Supplier will review and verify Supplier Personnel's continued need for access and level of access to Con Edison Information and Con Edison systems, networks and property on a quarterly basis. Documentation of the review will be provided by Supplier to Con Edison after the completion of each review.

(d) Notification and Revocation: Supplier will, before the end of the next Business Day following a change as described below, notify Con Edison by telephone and e-mail and will immediately take all steps necessary to remove Supplier Personnel's access to any Con Edison Information, systems, networks, or property when:

i. any Supplier Personnel no longer requires such access in order to furnish the goods or services provided by Supplier under the Contract,

ii. any Supplier Personnel is terminated or suspended or his or her employment is otherwise ended,

iii. Supplier reasonably believes any Supplier Personnel poses a threat to the safe working environment at or to any Con Edison property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or Con Edison Information,

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

v. any Supplier Personnel loses his or her U.S. work authorization, or

vi. Supplier's provision of goods and services to Con Edison under the Contract is either completed or terminated, so that Con Edison can discontinue electronic and/or physical access for such Supplier Personnel.

Supplier will take all steps reasonably necessary to immediately revoke such Supplier Personnel electronic and physical access to Con Edison Information as well as Con Edison 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 Supplier Personnel, Supplier will return to Con Edison any Con Edison-issued property including, but not limited to, Con Edison photo ID badge, keys, parking passes, documents, or electronic equipment in the possession of such Supplier Personnel. Supplier will notify the Con Edison authorized representative once access to Con Edison Information as well as Con Edison property, systems, and networks has been removed.

4. <u>Disclosure and Remediation by Vendors of Known Vulnerabilities Related to the Products or Services Provided to the Responsible Entity (Requirement R1.2.4)</u>

(a) Disclosure of Vulnerabilities by Contractor: Supplier shall develop and implement policies and procedures to address the disclosure and remediation by Supplier of vulnerabilities and material defects related to the goods and services provided to Con Edison under the Contract including the following:

i. Prior to the delivery of the procured goods or services, Supplier shall provide summary documentation of publicly disclosed vulnerabilities and material defects in the procured goods or services, the potential impact of such vulnerabilities and material defects, the status of Supplier's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Supplier's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

ii. Supplier shall notify Con Edison by telephone and e-mail of vulnerabilities and material defects in the procured goods or services within fifteen (15) days after such vulnerabilities and material defects become known to Supplier. Supplier shall provide summary documentation of vulnerabilities and material defects in the procured goods or services within sixty (60) calendar days after such vulnerabilities and material defects become known to Contractor. This includes notification of, and summary documentation on, vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the goods or services. 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.

iii. Supplier shall disclose the existence of all known methods, except as prohibited by law, methods for bypassing computer authentication in the procured goods or services, often referred to as backdoors, and provide written attestation that all such backdoors created by Supplier have been permanently remediated.

iv. Supplier shall implement a documented vulnerability detection and remediation program consistent with industry standards (e.g., ISO-27417 Vulnerability Disclosure, NIST Cybersecurity Framework v1.1 Reference RS.AN-5, NIST Special Publication 800-53 Rev. 4 RA-5, SA-11, and SI-2, as may be amended). Supplier shall provide the program to Con Edison for review upon Con Edison's request.

(b) Disclosure of Vulnerabilities by Con Edison: Whether or not publicly disclosed by Supplier and notwithstanding any other limitation in the Contract, Con Edison may disclose any vulnerabilities or material defects, and/or any other findings related to the goods and services provided by Supplier to: (i) the Electricity Information Sharing and Analysis Center, the United States Cyber Emergency Response Team ("CERT"), or any equivalent U.S. governmental entity or program, (ii) to any applicable U.S.

governmental entity when necessary to preserve the reliability of the BES as determined by Con Edison in its sole discretion, or (iii) any entity required by applicable law.

5. <u>Verification of Software Integrity and Authenticity of All Software and Patches Provided by the Vendor for Use in the BES Cyber System, and its associated EACMS and PACS (Requirement R1.2.5)</u>

(a) Hardware, Firmware, Software, and Patch Integrity and Authenticity:

i. Supplier shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under the Contract.

ii. Supplier shall specify how digital delivery for procured goods (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If Con Edison deems that it is warranted, Supplier shall apply encryption to protect procured goods throughout the delivery process.

iii. If Supplier provides software or patches to Con Edison, Supplier 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 Con Edison to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from Supplier's website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Supplier.

iv. Supplier shall use or arrange for the use of trusted channels to ship procured goods, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries

v. Supplier shall demonstrate chain-of-custody documentation for procured goods as determined by Con Edison in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

vi. Supplier shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

vii. Supplier shall identify or provide Company with a method to identify the country (or countries) of origin of the procured Supplier product and its components (including hardware, software, and firmware). Supplier will identify the countries where the development, manufacturing, maintenance, and service for the Supplier product are provided. Supplier will notify Con Edison of changes in the list of countries where product maintenance or other services are provided in support of the procured Supplier product. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.

(b) Patching Governance:

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

a. 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 Con Edison; and

b. the approach and capability to remediate newly reported zero-day vulnerabilities for the applicable Supplier goods or products.

ii. Unless otherwise approved by Con Edison in writing, the current or supported version of Supplier goods and services supplied by Supplier 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.).

iii. Supplier shall verify and provide documentation that procured goods (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to Con Edison.

iv. In providing the goods and services described in the Contract, Supplier shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for Supplier goods as soon as is practical. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within 7 days.

v. When third-party hardware, software (including open-source software), and firmware is provided by Supplier to Con Edison, Supplier shall provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses, if applicable to Con Edison's use of the third-party product in its system environment, as soon as is practical but not to exceed 30 days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, 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 Supplier within these time periods, Supplier shall provide or arrange for the provision of recommended mitigations and/or workarounds within sixty (60) days.

(c) Viruses and Firmware:

i. Supplier will use reasonable efforts to investigate whether Viruses are present in any software or patches before providing such software or patches to Con Edison. To the extent Supplier is supplying third-party software or patches, Supplier will use reasonable efforts to ensure the third-party investigates whether Viruses are present in any software or patches providing them to Con Edison or installing them on Con Edison's information networks, computer systems, and information systems.

ii. Supplier warrants that it has no knowledge of any Viruses coded or introduced into any software or patches, and Supplier 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 Supplier is supplying third-party software or patches, Supplier will use reasonable efforts to ensure the third-party 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.

iii. When install files, scripts, firmware, or other Supplier delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor, Supplier must provide or arrange for the provision of a technical explanation as to why the "false positive" hit has taken place to ensure their code's supply chain has not been compromised.

iv. If a Virus is found to have been coded or otherwise introduced as a result of Supplier's breach of its obligations under the Contract, Supplier shall promptly upon written request by Con Edison and at Supplier's own cost:

a. Take all necessary remedial action and provide assistance to Con Edison to eliminate the Virus throughout Con Edison's information networks, computer systems, and information systems, regardless of whether such systems or networks are operated by or on behalf of Con Edison; and

b. If the Virus causes a loss of operational efficiency or any loss of data (a) where Supplier is obligated under the Contract to back up such data, take all steps necessary and provide all assistance required by Con Edison and its affiliates, and (b) where Supplier is not obligated under the 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.

(d) Cryptographic Requirements:

i. Supplier shall document how the cryptographic system supporting the Supplier's goods and/or services procured under the 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:

a. The cryptographic methods and primitives that are implemented in the system, and how these methods are to be implemented.

b. The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

ii. Supplier 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.

iii. Supplier shall ensure that:

a. 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.

b. The key update method supports remote re-keying of all devices within 30 days as part of normal system operation.

c. Emergency re-keying of all devices can be remotely performed within 30 days.

iv. Supplier shall provide or arrange for the provision of a method for updating cryptographic primitives or algrorithms.

(e) <u>End of Life Operating Systems:</u>

i. Supplier-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.

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

6. <u>Coordination of Controls for vendor-initiated remote access (Requirement R1.2.6)</u>

Supplier shall coordinate with Con Edison on all remote access to Con Edison's systems and networks, regardless of interactivity, and shall comply with any controls for remote access sessions requested by Con Edison.

(a) Controls for Remote Access: Suppliers that directly, or through any of their affiliates, subcontractors or service providers, connect to Con Edison's systems or networks agree to the additional following protective measures:

i. Supplier will not access, and will not permit any other person or entity to access, Con Edison's systems or networks without Con Edison's written authorization and any such actual or attempted access will be consistent with any such written authorization.

ii. Supplier 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.

iii. Supplier shall ensure Supplier Personnel do not use any virtual private network or other device to simultaneously connect machines on any Con Edison system or network to any machines on any Supplier or third-party systems, without

a. using only a remote access method consistent with Con Edison's remote access control policies,

b. providing Con Edison 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

c. ensuring that any computer used by Supplier Personnel to remotely access any Con Edison system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Con Edison systems or networks.

iv. Supplier shall ensure credentials used to access Con Edison networks are not shared between Supplier Personnel.

7. General

(a) Supplier Cyber Security Policy: Upon request by Con Edison, Supplier will provide to Con Edison the Supplier's cyber security policy which shall be consistent with industry standard practice (e.g., NIST Special Publications 800-53 (Rev. 4) as may be amended). Supplier will implement and comply with its established cyber security policy. Any changes to Supplier's cybersecurity policy as applied to goods and services provided to Con Edison under the Contract or Con Edison Information shall not decrease the protections afforded to Con Edison or Con Edison Information and any material changes shall be communicated to Con Edison in writing by Supplier prior to implementation.

(b) Return or Destruction of Con Edison Information: Upon completion of the delivery of the goods and services to be provided under the Contract, or at any time upon Con Edison's request, Supplier will return to Con Edison all physical media (e.g., hardware, removable media) provided by Con Edison containing Con Edison Information. Con Edison Information in such physical media shall not be removed or altered in any way. The physical media should be physically sealed and returned via a bonded courier or as otherwise directed by Con Edison. If physical media containing Con Edison Information is owned by Supplier or a third-party, a notarized statement detailing the destruction method of the Con Edison Information used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated Con Edison security representative within fifteen (15) calendar days after completion of the delivery of the goods and services to be provided under the Contract, or at any time upon Con Edison's request. Supplier's destruction or erasure of Con Edison Information pursuant to this Section shall be in compliance with industry standard practices (e.g., Department of Defense 5220-22-M Standard, as may be amended).

(c) Compliance; Audit Rights: Upon request, Supplier shall provide to Con Edison the opportunity to review a copy of Supplier's policies, procedures, evidence and independent audit report summaries that are part of a cyber security framework (e.g., ISO-27001, SOC2). Con Edison or its third-party designee may, but is not obligated to, perform audits and security tests of Supplier's information technology or systems environment and procedural controls to determine Supplier's compliance with the system, network, data, and information security requirements of the Contract. Con Edison audits of the Supplier system shall be done with at least 30 days advance notice. These audits and tests may include coordinated security tests as mutually agreed to not unduly affect Supplier operations, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use, retention, and authorized destruction of Con Edison Information. Supplier shall provide all information reasonably requested by Con Edison in connection with any such audits and shall provide reasonable access and assistance to Con Edison upon request. Supplier will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. Con Edison reserves the right to view, upon request, any original security reports that Supplier has undertaken or commissioned to assess Supplier's own network security. If requested, copies of these reports will be sent via bonded courier to a designated Con Edison security representative. Supplier will notify Con Edison of any such security reports or similar assessments once they have been completed. Without limiting the terms of paragraph (d) immediately below, any regulators of Con Edison or its affiliates shall have the same rights of audit as described herein upon request.

(d) Regulatory Examinations: Supplier agrees that any regulator or other governmental entity with jurisdiction over Con Edison and its affiliates may examine Supplier's activities relating to the performance of its obligations under the Contract to the extent such authority is granted to such entities under the law. Supplier shall promptly cooperate with and provide all information reasonably requested by the regulator or other governmental entity in connection with any such examination and provide reasonable assistance and access to all equipment, records, networks, and systems reasonably requested by the regulator or other governmental entity. Supplier agrees to comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes at Supplier's sole cost and expense. The foregoing cooperation and assistance will be rendered at Supplier's then-current time and materials rates, subject to Con Edison's prior written authorization.