Edison Electric INSTITUTE

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

Version 4.0

June 2026

DISCLAIMER

This work was prepared by a committee of representatives of EEI member companies to facilitate managing cybersecurity supply chain risks during procurement. EEI, any member of EEI, and any person acting on its behalf (a) does not make any warranty, express or implied, with respect to the accuracy, completeness or usefulness of the information, advice or recommendations contained in this work, and (b) does not assume and expressly disclaims any liability with respect to the use of, or for damages resulting from the use of any information, advice or recommendations contained in this work. By providing this work, EEI does not offer legal advice and all users are urged to consult their own legal counsel to ensure that their security objectives will be achieved, and their legal interests are adequately protected.

Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk

On October 18, 2018, the Federal Energy Regulatory Commission ("FERC") approved the North American Electric Reliability Corporation ("NERC") Reliability Standard CIP-013-1 (Cyber Security—Supply Chain Risk Management). The Reliability Standard supplements the current NERC Critical Infrastructure Protection ("CIP") Standards to mitigate cybersecurity risks associated with the supply chain for grid-related cyber systems. The CIP-013-1 Reliability Standard became effective on October 1, 2020. Since then, CIP-03-2 became effective on October 1, 2022, and CIP-013-3 will take effect on July 1, 2028.

CIP-013-2 Requirement R1 directs Responsible Entities to "develop one or more documented supply chain cyber security risk management plan(s)" that include processes to use in Bulk Electric System ("BES") Cyber System procurement that will require vendor cooperation to protect the security of the BES Cyber System supply chain. Responsible Entities will address these requirements by, among other means, inserting contract terms that address the R1.2 security controls in agreements with vendors. The model procurement contract language contained in this document targets the processes required in CIP-013-2 Requirement R1.2 as well as supporting contract terms that address related information and data protection to strengthen cybersecurity overall.

The model procurement contract language below provides Registered Entities a consistent set of provisions to address CIP-013-2 security controls within their own respective contractual forms. However, as noted in the Technical Rational for CIP-013-2, "[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity's plan."

Version 4.0

The *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk*, originally released in March 2019, was updated with Version 2.0 in May 2020, Version 3.0 in October 2022, and Version 4.0 in June 2026 to reflect evolving industry approaches, adjust notification timeframes and other time-specified requirements, modify language where appropriate to clarify existing concepts, and address new concepts such as cloud security requirements and artificial intelligence. EEI greatly appreciates the work of the EEI members and other partners who participated in this update process.

Definitions

The following definitions apply only to the terms and conditions in this [Exhibit/Attachment].

"Access Control Policy" means policies and procedures to address the security of Contractor's remote and onsite access to Company Information, Company systems and networks, and Company property.

"**AI Services**" should include both the desired deliverables and the intended use of the AI tools and technology.

"AI Systems" AI Technology that is owed or licensed by Contractor and made available to Company for use in connection with this Agreement.

"**AI Technology**" means any and all machine learning, deep learning, and other artificial intelligence ("AI") technologies or systems, including statistical learning algorithms, models (including large language models), neural networks, and other AI tools or methodologies, all software implementations of any of the foregoing, and related hardware or equipment capable of generating various types of content (including, but not limited to, data analysis, text, images, video, audio, or computer code) based on user-supplied prompts or inputs.

"**CEII**" means Critical Energy Infrastructure Information and/or Critical Electric Infrastructure Information.

"**Company**" means the organization that acquires or procures a product or service.

"**Company Information**" means for purposes of these terms and conditions, any and all data and other information concerning Company and its business in any form, including, without limitation, the products and services provided under this Agreement that is disclosed to or otherwise learned by Contractor during the performance of this Agreement.

"**Company Confidential Information**" means for purposes of these terms and conditions, all non-public information concerning Company that has a restricted and internal need to know, the unauthorized disclosure of which could reasonably be expected to harm the Company.

"**Contractor**" or "**Vendor**" or "**Supplier**" means the organization or individual that enters into an agreement with the Company for supplying a product or service.

"**Contractor Proprietary Information**" means any Contractor information that is identified as highly confidential where disclosure outside of the Company may result in significant loss of Contractor's intellectual property, PII, etc. and may cause damage to the operational effectiveness or otherwise substantially disrupt significant business operations, with examples including but not limited to: source code and private encryption keys.

"**Data**" means any Company Information exchanged through the execution or performance of this Agreement.

"**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 (including without Company's consent), or for any unauthorized purpose.

"**Input Data**" means Data provided by Company to train, test, or use the AI. Company retains all ownership of Data provided to Contractor.

"Output/Generated Content" means results produced by the AI Technology based on Input Data including, without limitation: data, text, images, or insights.

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

"Prompts" means instructions or queries given to the AI Technology.

"**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 that may affect the Company Information or that could pose a cyber security risk to the Company ; or (iii) Contractor receives any third-party 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 Agreement or applicable laws; in connection with Company Information or (B) a verified impact to the cybersecurity of the products and services provided to Company that could pose a cybersecurity risk to the Company.

"**Senior Executive**" means any employee or officer of the Company who holds a title of Vice President or above, or who otherwise has a significant managerial, strategic, or decision-making authority.

"**Training Data"** means any and all information, data, materials, text, prompts, images, and other content that is used to train, retrain, validate, test, tune, retune, affect, improve, or improve Data used to train, the AI model.

"**Vulnerability**" means a weakness or defect in an information system, system security procedures, internal controls, firmware, software, or implementation that has resulted, continues to result in, or could result in a Security Incident including but not limited to being exploited or triggered by a threat source.

Requirement R1.2.1

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.

EEI Model Procurement Contract Language

Contractor agrees to notify Company (consistent with Company policy) in writing sent to [email address] immediately after Contractor's actual knowledge or reasonable belief of an occurrence of a Security Incident.

The written 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 summary of the facts and circumstances of the Security Incident, including a description, to the extent known, of a) why the Security Incident occurred (e.g., a description of the reason for the system failure), (b) the amount and nature of Company Information known or reasonably believed to have been Disclosed (if applicable), and (c) the measures being taken to address and remedy the Security Incident and to prevent the same or a similar event from occurring in the future. If the Contractor has filed a report relating to a security incident with any state or federal agency, the Contractor will notify the Company within 24 hours that the incident report was filed. To the extent it is not prohibited, the Company should provide a copy of the filed incident report. In the event Contractor is required by law enforcement to withhold such notification, Contractor is under no obligation to notify Company until such withholding is no longer required.

If such written notice is provided in the preceding paragraph, Contractor shall provide written updates to the initial written 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's efforts to determine the risk posed by the Security Incident to Company Information and Company assets.-Contractor shall retain information relating to the written notice and underlying Security Incident consistent with Contractor's data retention policy but in no event for a period no less than three years.

Requirement R1.2.2

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.

EEI Model Procurement Contract Language

Development and Implementation of a Response Plan: Contractor 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. Contractor shall provide Company with an opportunity and access to inspect Contractor's Response Plan, provided that Contractor shall have a right to redact any part of the Response Plan that contains Contractor Proprietary Information or information protected by legal privilege. The Contractor's Response Plan should be updated at least annually, or as needed.

The development and implementation of the Response Plan shall follow industry standard practices, such as those that at a minimum are consistent with the current released versions of 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.

Prevention of Recurrence: If the Security Incident arises from Contractor-provided software, hardware, or equipment, then, within [insert number] days of a Security Incident, Contractor shall develop and take necessary steps to execute mitigation measures that reduce 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 to Company the implementation of the mitigating measures to reduce a similar Security Incident. If the Security Incident arises from a third-party supplier's software, equipment or services, then if Contractor is permitted to disclose such information, Contractor shall provide updates to Company of such third-party supplier's plan for the prevention of recurrence of such Security Incident. Except to the extent publicly available, any information provided hereunder by Contractor shall be treated as confidential and not disclosed to any third party without Contractor's prior written approval, unless required by applicable governmental entities.

Coordination of Incident Response with Company:

(a) Contractor will, at its sole cost and expense, assist and cooperate with Company with respect to any investigation of and response to a Security Incident including disclosures to affected parties in connection with a Security Incident or any required response or disclosure directed by applicable laws related to a Security Incident.

(b) In the event a Security Incident stems from or results in Company Information being disclosed, Company will have sole control over the timing and method of providing notification as required

Requirement R1.2.3

Notification by vendors when remote or onsite access should no longer be granted to vendor representatives.

EEI Model Procurement Contract Language

Development and Implementation of Access Control Policy: Contractor shall develop 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-2,10 PE-2,11 PS4,12 and PS-5 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 (collectively, "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 three years from the date of each review. Contractor will also review and verify Contractor Personnel's continued need for access and level of access when job responsibilities change.

Notification and Revocation: Contractor will promptly notify Company, but no later than [negotiated timeframe] (hour(s)) when any of the circumstances enumerated below occur (and, if any such required notification should occur outside of normal business hours, Contractor will provide notice to the Company's 24 x 7 notification line, available at (Insert contact information), or other agreed upon method between Company and Contractor):

(i) any Contractor Personnel no longer requires such access in order to furnish the services or products provided by Contractor under this Agreement,
(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 Agreement is either completed or terminated, so that Company can discontinue electronic and/or physical access for such Contractor Personnel.

Should any such circumstance occur, Contractor will take all steps reasonably necessary to immediately revoke such Contractor Personnel's 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 badges, keys, parking passes, documents, or electronic equipment in the possession of such Contractor Personnel. Contractor will notify Company at [insert contact information] once access to Company Information as well as Company property, systems, and networks has been removed.

Requirement R1.2.4

Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity.

EEI Model Procurement Contract Language

Contractor shall develop and implement policies and procedures to address the disclosure by Contractor of known Vulnerabilities related to the products and services provided to Company under this Agreement including the following:

(a) Prior to the delivery of the procured product or service, Contractor shall disclose known Vulnerabilities. Contractor shall provide or direct Company to an available source of summary documentation of Vulnerabilities in the procured product or services, the potential impact of such Vulnerabilities, 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 in the procured product or services within thirty (30) calendar days after any such Vulnerabilities become known to Contractor, consistent with ISO/IEC 30111 and 29147 for Coordinated Vulnerability Disclosure. The summary documentation shall include a description of each Vulnerability 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-27417 Vulnerability Disclosure, NIST Cybersecurity Framework v1.1 Reference RS.AN-5, NIST Special Publication 800-53 Rev. 4 RA-5,17 SA-11,18 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 Agreement, following Company's reasonable written notice provided to and acknowledged by Contractor, Company may disclose any Vulnerabilities and/or other findings related to the products and services provided by Contractor to (a) the Electricity Information Sharing and Analysis Center ("EISAC"), 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 Bulk Electric System (BES), or (c) any entity required by applicable law.

Requirement R1.2.5

Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System.

EEI Model Procurement Contract Language

Hardware, Firmware, Software, and Patch Integrity and Authenticity:
(a) Contractor shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under this Agreement, in accordance with industry standards. 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 for [negotiated time period] spare parts shall be made available by Contractor.

(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 is delivered in accordance with Company data encryption policy or procedure. When product features and delivery mechanisms allow, 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 verification.

(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 country of manufacture (hardware) and country of build (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 shall be in writing and 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 provide chain-of-custody documentation for procured products appropriate to scope of supply.

Patching Governance:

(a) Prior to the delivery of any products and/or services to Company or any connection of electronic devices, assets, or equipment to Company's electronic equipment, Contractor shall provide documentation regarding the patch management and vulnerability management/mitigation programs and shall update Contractor's patch management and vulnerability management/mitigation processes (including for any third-party hardware, 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 Agreement. 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, products and services supplied by Contractor shall not require the use of any out-of-date, unsupported, or end of-life version of third-party components (e.g., Java, Flash, Web browser, etc.), unless information is provided in a Bill of Materials or other method.

(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 supplying any product or service to the Company.

(d) In providing the products and services described in this Agreement, Contractor shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered Vulnerabilities for Contractor products within [a negotiated time period] days. Updates to remediate Vulnerabilities shall be provided within a shorter period than other updates, within [a negotiated time period (e.g., 7, 14, or 21 days)]. If updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations, methods of exploit detection, and/or workarounds within [a negotiated time period].

(e) In providing third-party hardware, software (including open-source software), and when firmware is provided by Contractor to Company, Contractor shall provide or arrange for the appropriate hardware, software, and/or firmware updates to remediate newly discovered Vulnerabilities, if such Vulnerabilities are applicable to the Company's use of the third-party product in its system environment, within 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 updates, within [a negotiated time period (e.g., 30, 60, or 90 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 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 by Contractor to Company or installed by Contractor 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 which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

(c) When install files, scripts, firmware, or other Contractor-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, Contractor must provide or

arrange for the provision of technical justification as to why the "false positive" hit has taken place to ensure the flagged product 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 performance under this Agreement, Contractor shall upon written request by Company and at Contractor's own cost:

(i) Take all commercially reasonable action 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 Agreement to back up such Data, take all commercially reasonable steps necessary and provide all assistance required by Company and its affiliates, or (B) where Contractor is not obligated under this Agreement 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) As mutually agreed, Contractor-delivered solutions will not be required to reside on end-of-sale, end-of-support, and end-of-life operating systems, or any operating system that is known to be reaching such status six (6) months from the date of installation.

(b) As mutually agreed, 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 Agreement 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, ongoing 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) As mutually agreed, 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) As mutually agreed, 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) As mutually agreed, the key update method supports remote re-keying of all devices within [a negotiated time period(s)] as part of normal system operations.
(iii) Emergency re-keying of all devices can be performed remotely or on-site within 30 days. (e) Contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

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

Requirement R1.2.6

Coordination of controls for (i) vendor-initiated interactive remote access, and (ii) system-to-system remote access with a vendor(s).[1]

EEI Model Procurement Contract Language

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,

[1] Please note that although this language is broader than the actual text of Requirement R1.2.6,, it tracks the text of the associated Technical Rationale for Requirement R1.2.6.

(ii) 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 or among Contractor Personnel.

EEI Model Procurement Contract Language Supporting Provisions

CLOUD SECURITY REQUIREMENTS

In support of this Agreement, if Contractor will use cloud computing services which will require storage of, access to or transmission of Company Information, Contractor must comply with the following requirements.

Contractor or sub-Contractor's cloud infrastructure which hosts or transmits Company Data must be geographically located within the United States and must not be transmitted to devices in any country other than the United States.

Before access to Company Data is granted, Contractor must:

- Provide Company with a general description of the cloud computing services used to support Contractor and the intended use(s).
- Provide evidence of the controls, processes, and procedures to maintain confidentiality, integrity, and availability of Data stored in the cloud.
- Provide documentation demonstrating the ability for Company to completely delete Company Data and demonstrate that Company Data is inaccessible after deletion.
- Provide Company with notice if there is a material change in ownership of Contractor.

Regarding the use of Company Data:

- Contractor must provide the option of an encryption key to Company.
- Contractor must provide Company with exclusive control of access management to Company Data.
- Company Data stored or transmitted by Contractor must be encrypted in transit and at rest.
- All personnel who support Contractor's cloud infrastructure shall be in the United States and undergo a background investigation.
- Any third-party Contractor supporting Contractor's cloud solution must undergo a background investigation prior to access approval.
- Contractor must complete Company's security risk assessment questionnaire and be in good standing prior to implementation of Contractor's cloud solution.

- Contractor and Contractor's cloud service contractor shall promptly respond to Company's information requests regarding Contractor or Contractor's cloud service contractor, Contractor's cloud service infrastructure, controls, processes, procedures and support personnel as necessary for Company to comply with regulatory and security audits.

ARTIFICIAL INTELLIGENCE

General Provisions:

- Contractor will provide Company with a general description of the AI Technology used to support this Agreement, and the intended use(s).
- Contractor or sub-Contractor's AI Technology which hosts or transmits Company Data must be geographically located in the United States and must not be transmitted to devices in any country other than the United States.
- Contractor's use of the AI Technology will not result in any Company Data or work product created for Company being used as Training Data without Company's express written consent.
- Contractor has not used any AI Technology in a manner that has, does, will, or could reasonably be expected to limit or adversely affect Company's rights.
- Contractor shall identify a single Senior Executive who has responsibility for secure use of AI Technology.
- In the event the Contractor is using Company Data, Contractor personnel with authorized access shall identify the party within the Company with responsibility for handling such Company Data and establish a direct line of communication with such party.

Contractor's AI Systems for Company Use:

- Contractor grants Company a fully paid up, nonexclusive license during the term of the Agreement to use the AI Systems, including all Training Data, and underlying algorithms.
- Company retains all right, title, and interest, in and to all Input Data and Output/Generated Content related to Company's use of the AI Systems.

On Use of Company Data:

- Contractor will not input, insert, share, or transmit any Company Information to any commercially available artificial intelligence software or technology, applications, tools, equipment or platforms or other AI Technology that inputs data into a shared or public database for any purposes, or that inputs data into any privately available database that is used to provide services to parties other than Company, without first receiving Company's express written consent.
- Contractor shall not use any Input Data used by Company with the AI Systems or Output/Generated Content generated by Company using the AI Systems as Training

Data for any AI Technology, including the AI Systems, without first receiving Company's express written consent.

- Contractor may utilize Company Information with generative AI instances that are utilized exclusively to provide services to Company in conformance with this Agreement. In doing so, Company Information must be supported by a separately segregated instance of the service or environment that is dedicated to Company.
- Contractor will make itself available to Company at least annually to discuss how aggregated or anonymized Company Data is used to inform internal Contractor AI Technology.
- Contractor will ensure that the AI Systems are in material compliance with industry standard practices for the ethical and responsible use of AI Technology.
- Contractor will ensure that the AI Systems cannot be used, and Contractor shall not use or allow AI Systems to be used, to extract non-anonymized personal data (as defined under relevant data protection laws); and,
- Contractor will ensure that any personal data (as defined under relevant data protection laws) used as Training Data for the AI Systems is lawfully processed.

Company Approval of Contractor's Use of AI Technology:

- Contractor shall disclose to Company all AI Technology Contractor may utilize to perform the AI Services, including commercially available AI Technology, and enumerate the same to Company in a list as part of this Agreement. This list shall be updated annually or as material changes dictate.
- Contractor shall not use any AI Technology in the provision of AI Services without the prior written consent of Company.
- Contractor agrees that any AI Technology that will handle Company Data must go through the Security and Technology review process, and any tool approved for use will be subject to ongoing testing and monitoring as defined by Company.

Intellectual Property:

- Contractor warrants that its use of AI Technology used in the performance of AI Services will not infringe upon or violate any trademarks, patents, copyrights, trade secrets or other third-party intellectual property rights or other rights. If the performance of AI Services is held in any action to constitute infringement or violation of the forgoing, or the use of the AI Services is enjoined for such reasons, Contractor, at its expense, shall procure for Company the right to continue use of the AI Services, or replace the AI Services with non-infringing (or violating) materials or methods satisfactory to Company, or modify the AI Services in a manner satisfactory to Company so that the AI Services become non-infringing (or non-violating).
- Contractor agrees to indemnify and hold Company harmless from and against any and all claims, liability, losses or damages, including attorneys' fees, arising out of or related any alleged infringement or violation of third-party rights contemplated above.

Breach Disclosure:

- In the event Contractor discovers or becomes aware of a breach of access to AI Technology, or any unauthorized change to underlying algorithms used in AI Technology, Contractor will pause use of such AI technology in support of this Agreement and inform Company immediately.

The **Edison Electric Institute** (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide safe, reliable electricity for nearly 250 million Americans, and operate in all 50 states and the District of Columbia. Collectively, the electric power industry supports more than 7 million jobs in communities across the United States and drives economic growth and prosperity. EEI also includes hundreds of industry suppliers and related organizations as Associate Members.

Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums.

For more information, visit our Web site at **www.eei.org**.

Edison Electric Institute
701 Pennsylvania Avenue, NW
Washington, DC 20004-2696
202-508-5000 | www.eei.org