© 2019 by the Edison Electric Institute (EEI). All rights reserved. Published 2019. Printed in the United States of America. Automatic License – Permission of the copyright owners is granted for reproduction by downloading from a computer and printing electronic copies of the work. No authorized copy may be sold. The industry is encouraged to use this work in its transactions. Attribution to the copyright owners is requested.

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


CIP-013-1 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-013-1 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-013-1 security controls within their own respective contractual forms. However, as noted in the Guidelines and Technical Basis for CIP-013-1, “[o]btaining specific controls in the negotiated contract may not be feasible and is not considered failure to implement an entity’s plan.”

Definitions

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

“Contractor” means the organization or individual that enters into an agreement with Company for supplying a product or service.

---

1 See Supply Chain Risk Management Standard, Order No. 850, 165 FERC ¶ 61,020 (2018); NERC proposed the CIP-013-1 Reliability Standard on September 18, 2016 in response to a FERC directive in Revised Critical Infrastructure Protection Reliability Standards, Order No. 829, 156 FERC ¶ 61,050, at P 43 (2016).

2 Contract terms are a direct means for Responsible Entities to secure vendor cooperation, a concept that FERC acknowledged in its initial directive. See Order No. 829 at P 59 (“The new or modified Reliability Standard must address the provision and verification of relevant security concepts in future contracts for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations.”)

3 ESCSWG, Cybersecurity Procurement Language for Energy Delivery Systems at Table 1 (Apr. 2014) (“ESCSVWG Procurement Guidance”). Also note, the CIP-013-1 Reliability Standard uses the term “vendor”. The procurement contract language presented herein follows common industry practice of using the term “contractor.” In this context, the terms “vendor” and “contractor” are intended to have the same meaning.
“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 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.

“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.

“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) Contractor’s handling of Company Information or Contractor's compliance with the data safeguards in this Agreement or applicable law in connection with Company Information or (B) the cybersecurity of the products and services provided to Company by Contractor.

**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 immediately at [insert contact telephone, email address, and physical address] by telephone and email, and subsequently via written letter, whenever a Security Incident occurs.

The 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 precise 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.

---

4 ESCSWG Procurement Guidance, Table 1.
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 cooperate with Company in Company’s efforts to determine the risk to the BES posed by the Security Incident, including providing additional information regarding the Security Incident upon request from Company.

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 policies and procedures to address Security Incidents (“Response Plan”) by mitigating the harmful effects of Security Incidents and addressing andremedying 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 best practices 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.

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 of that implementation by contacting [insert contact name].

---

5 Language based on 45 C.F.R. § 164.308(a)(6)(i) and (ii).
Prevention of Recurrence: Within [number of] 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 NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, as may be amended,\(^9\) 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.

Coordination of Incident Response with Company: Within [insert number of] days of notifying Company 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. Contractor shall coordinate with Company in developing those action plans and mitigating controls. Contractor will provide Company guidance and recommendations for long term remediation of any cyber security risks posed to Company Information, equipment, systems, and networks as well as any information necessary to assist Company in any recovery efforts undertaken by Company in response 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’s confidential information 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 or may reasonably compromise the cybersecurity of the products and services provided by Contractor to an entity other than Company; or (c) Contractor receives any complaint, notice, or communication which relates directly or indirectly to (i) Contractor’s handling of confidential information or Contractor's compliance with applicable

---

law in connection with confidential 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 (1) why the Unrelated Security Incident occurred, (2) the nature of the confidential information disclosed, and (3) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

**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 and implement policies and procedures to address the security of remote and onsite access to Company Information, Company systems and networks, and Company property (an “Access Control Policy”) that is consistent with the personnel management requirements of NIST Special Publication 800-53 Rev. 4 AC-2, PE-2, PS-4, 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 (“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

---

10 AC-2 covers Account Management.
12 PS-4 covers Personnel Termination.
13 PS-5 covers Personnel Transfer.
systems, networks and property on a semi-annual basis and will retain evidence of the reviews for two years from the date of each review.

**Notification and Revocation:** Contractor will immediately notify Company in writing (no later than close of business on the same day as the day of termination or change set forth below) and will immediately take all steps necessary to remove Contractor Personnel’s access to any Company Information, systems, networks, or property when:

(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 employee 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 fails to maintain conduct in accordance with the qualification criteria set forth in __________,\(^{14}\)

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

(vii) 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.

Contractor will take all steps reasonably necessary to immediately deny 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, RSA tokens, and laptops, as applicable, and will return to Company any Company-issued property including, but not limited to, Company photo ID badge, keys, parking pass, documents, or laptop 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.

\(^{14}\) Insert cross reference(s) to Section(s) of contract that set forth Contractor personnel qualification criteria.
### Requirement R1.2.4

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

### EEI Model Procurement Language

Contractor shall 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 Agreement including the following:

(a) Prior to the delivery of the procured product or service, Contractor shall provide 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 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. This includes summary documentation on vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the product. 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.

(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 documentation that all such backdoors created by Contractor have been permanently deleted or disabled.

(d) Contractor shall implement a vulnerability detection and remediation program consistent with NIST Special Publication 800-53 Rev. 4 RA-5, 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 Agreement, Company may disclose any

---

15 Based on language in ESCSWG Procurement Guidance § 3.2.1.
16 Based on language in ESCSWG Procurement Guidance § 3.2.2.
17 Based on language in ESCSWG Procurement Guidance § 2.1.5.
18 RA-5 covers Vulnerability Scanning.
20 SI-2 covers Flaw Remediation.
vulnerabilities or material defects in the products and services provided by Contractor to (a) the Electricity Information Sharing and Analysis Center, the Industrial Control Systems Cyber Emergency Response Team, or any equivalent entity, (b) to any 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.

**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.

**Proposed EEI 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. 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, commitment to ensure that for [a 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 as specified. If Company deems that it is warranted, Contractor shall apply encryption to protect procured products throughout the delivery process.

(i) 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 and avoid downloading the software or patches from Contractor’s website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Contractor.

(c) Contractor shall identify the country (or countries) of origin of the procured product and its components (including hardware, software, and firmware). Contractor will identify the countries where the development, manufacturing, maintenance, and service for the 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 product. This notification shall occur 180 days prior to initiating a change in the list of countries.
(d) Contractor shall use trusted channels to ship procured products, such as U.S. registered mail.

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

(f) 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.\(^{21}\)

**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 hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required 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 Contractor’s method or recommendation for how the integrity of a patch is validated by Company; and

(ii) Contractor's approach and capability to remediate newly reported zero-day vulnerabilities.

(b) Unless otherwise approved by the Company in writing, current or supported version of Contractor products and services 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 Agreement Contractor shall provide appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated time period]. Updates to remediate critical 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 and/or workarounds within [a negotiated time period].

\(^{21}\) Based on language in ESCSWG Procurement Guidance § 3.6.
(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 firmware updates to remediate newly discovered vulnerabilities or weaknesses within [a negotiated time period]. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within [a negotiated time period (e.g., 30, 60, or 90 days)]. If these third-party updates cannot be made available by Contractor within these time periods, Contractor shall provide mitigations and/or workarounds within [a negotiated time period].

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.

(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.

(c) When install files, scripts, firmware, or other Contractor delivered software solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor through open source solutions like “Virus Total,” Contractor must provide technical proof as to why the “false positive” hit has taken place to ensure their 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 result of Contractor’s breach of its obligations under this Agreement, Contractor shall immediately 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, regardless of whether such systems or networks are operated by or on behalf of Company; 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 steps necessary and provide all assistance required by Company and its affiliates, and (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) 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 protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system as specified by Company. 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) Contractor shall provide 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 [a negotiated time period(s)] as part of normal system operations.

   (iii) Emergency re-keying of all devices can be remotely performed within [a negotiated time period (e.g., 30 days)].

(e) Contractor shall provide a method for updating cryptographic primitives or algorithms.\(^{22}\)

\(^{22}\) Based on language in ESCSWG Procurement Guidance § 7.
### 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).

### Proposed EEI 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 authorization and any such actual or attempted access will be consistent with any such 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,

   (ii) 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.
Supporting Provisions

EEI Model Procurement Contract Language

Contractor Cybersecurity Policy: Contractor will provide to Company the Contractor’s cybersecurity policy, which shall be consistent with NIST Special Publication 800-53 (Rev. 4) as may be amended. Contractor will implement and comply with that cybersecurity policy. Any changes to Contractor’s cybersecurity policy as applied to products and services provided to Company under this Agreement and Company Information that are inconsistent with the security requirements of NIST Special Publication 800-53 (Rev. 4) as may be amended shall be subject to review and approval by Company prior to implementation by Contractor.

Return or Destruction of Company Information: Upon completion of the delivery of the products and services to be provided under this Agreement, or at any time upon Company’s request, Contractor will return to Company all hardware and removable media provided by Company containing Company Information. Company Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by Company. If the hardware or removable media containing Company Information is owned by Contractor or a third-party, a notarized statement detailing the destruction method 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 Company security representative within fifteen (15) calendar days after completion of the delivery of the products and services to be provided under this Agreement, or at any time upon Company’s request. Contractor’s destruction or erasure of Company Information pursuant to this Section shall be in compliance with best industry practices (e.g., Department of Defense 5220-22-M Standard, as may be amended).

Audit Rights: Company or its third-party designee may, but is not obligated to, perform audits and security tests of Contractor’s IT or systems environment and procedural controls to determine Contractor’s compliance with the system, network, data, and information security requirements of this Agreement. These audits and tests may include coordinated security tests, 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 Company Information. Contractor shall provide all information reasonably requested by Company in connection with any such audits and shall provide reasonable access and assistance to Company upon request. Contractor will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. Company reserves the right to view, upon request, any original security reports that Contractor has undertaken or commissioned to assess Contractor’s own network security. If requested, copies of these reports will be sent via bonded courier to Company security contact. Contractor will notify Company of any such security reports or similar assessments once they have been completed. Any regulators of Company or its affiliates shall have the same rights of audit as described herein upon request.
Regulatory Examinations: Contractor agrees that any regulator or other governmental entity with jurisdiction over Company and its affiliates may examine Contractor’s activities relating to the performance of its obligations under this Agreement to the extent such authority is granted to such entities under the law. Contractor 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. Contractor agrees to comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes at Contractor’s sole cost and expense. The foregoing cooperation and assistance will be rendered at Contractor’s then-current time and materials rates, subject to Company’s prior written authorization.
The **Edison Electric Institute** (EEI) is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 65 international electric companies with operations in more than 90 countries, as International Members, and 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](http://www.eei.org).