**NERC CIP-013 REQUIREMENTS**

Upon execution of the Purchase Order by and between you and San Diego Gas & Electric Company (“**Company**”) for hardware (which may include embedded software) or other equipment (collectively, “**Equipment**”), these additional terms and conditions shall be incorporated therein. These obligations and requirements shall not reduce or otherwise limit any obligations set forth in the Purchase Order or any controlling master agreement. The references set forth herein (e.g., R1.2.2) concern NERC CIP-013 and are for convenience and reference only.

1. Response Plan.

You shall develop and implement policies and procedures to address a Security Incident (“**Response Plan**”). A “**Security Incident**” shall mean any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise (i) the cybersecurity of your Equipment; or (ii) the physical, technical, administrative, or organizational safeguards put in place by you that relate to the cybersecurity contemplated in (i) hereof. In addition, the Response Plan shall require your cooperation with Company in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise requested by Company. See R1.2.2.

1. Notice and Incident Response.
	1. Notice to Company. You shall notify the Sempra Energy Security Operations Center (SOC@sempra.com (858) 613-3278) as soon as possible, but no later than twenty-four (24) hours after becoming aware, of an internal or external Security Incident or possible Security Incident. Such notification shall include mitigation efforts to the extent they are not described in the Response Plan. See R1.2.1.
	2. Notice to Third Party. If a Security Incident requires notification to any third party, Company will have sole control over the timing, content and method of providing such notification.
	3. Incident Response Coordination. Within ten (10) business days of the completion of the Security Incident investigation, you shall provide recommended actions, including mitigation controls, to be taken by Company on Company control systems to reduce the risk of a recurrence of the same or a similar Security Incident. In addition, you shall make available all relevant records, logs, files, data reporting, and other materials to assist Company in any recovery efforts undertaken by Company. See R1.2.1 and R1.2.2.
2. Access Restrictions.

You shall (i) not permit your employees or anyone operating on your behalf to access Company’s property, systems, or networks except to the extent required for installation the Equipment and (ii) take all necessary action(s) to immediately remove access to the Company’s property, network, or systems (and immediately, notify Company in writing of such removal) upon such installation of the Equipment.

1. Supply Chain Standards; Hardware, Firmware, Software, and Patch Integrity.

You shall establish, document, and implement appropriate risk management practices for supply chain delivery of the Equipment (including patches, enhancements, updates, or upgrades, the “**Supply Chain Documentation**”). The Supply Chain Documentation shall include, without limitation, your chain of custody practices, inventory management, encryption methods to ensure digital delivery remains as specified and set forth in the Purchase Order. In addition, you shall publish or provide a hash satisfying the requirements of the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules 140-2 (or its successor standard) for software or patches provided to Company hereunder (collectively, “**Patches**”). If such hash is unavailable, you shall provide similar standard information on the Patches to enable Company to independently verify the integrity of the Patches. See R1.2.5.

1. Viruses.

You expressly warrant to Company that it will use its best efforts to ensure that no computer viruses, malware, or similar items are introduced into Company’s computing and network environment by the Equipment or Patches.

1. Vulnerabilities and Defects.

You, at your sole expense, shall maintain a vulnerability and defect tracking and remediation process which (i) reviews potential vulnerabilities and defects, that may or may have not been publicly disclosed, for their security impact to the Equipment, and (ii) tests and remediates all software vulnerabilities posted to the National Vulnerability Database (<http://nvd.nist.gov/>) and by Open Web Application Security Project ([www.owasp.org](http://www.owasp.org)) within thirty (30) days of such software vulnerabilities being posted. In addition, you shall disclose any such vulnerabilities or defects to Company and provide documentation detailing such vulnerabilities or defects contemplated in the preceding sentence to Company, including your efforts to mitigate those vulnerabilities or defects, and your recommended actions, compensating security controls, mitigations, and/or procedural workarounds, at no cost, to Company. See R1.2.4.

1. Conflicts.

Nothing contained herein shall be construed to limit any of your obligations regarding nondisclosure or information protections contained elsewhere in the Purchase Order or the controlling master agreement.