Critical Infrastructure Protection Requirements Exhibit

1. Applicability of Section:

   In addition to Contractor’s obligations under the Terms and Conditions:

   Unless instructed otherwise by Edison, Contractor must also comply with the requirements of these Critical Infrastructure Protection Requirements if any of the following circumstances apply:

   (a) Contractor is providing, or will provide, Edison with any NERC CIP Cyber Assets (identified as such by Edison) or portion thereof.

   (b) Contractor has, or will have, access, electronic or physical, to any NERC CIP Cyber Assets, Electronic Security Perimeters or Physical Security Perimeters (identified as such by Edison).

   (c) Contractor has, or will have, access to any NERC CIP Confidential Information (identified as such by Edison).

   (d) Contractor is providing, or will provide, a Service in connection with Edison’s compliance with the NERC CIP Standards (identified as such by Edison).

2. NERC CIP Overview:

   As part of the national electrical grid, Edison is mandated to comply with the North American Electric Reliability Corporation (“NERC”) Cyber Security Standards, also known as Critical Infrastructure Protection (“CIP”) Standards 002 through 009, which can be found at www.nerc.com (as may be modified or amended from time to time, “NERC CIP Standards”). These NERC CIP Standards focus on the physical and electronic security of Critical Cyber Assets and facilities that, if compromised, would have a significant impact upon Edison’s ability to serve the electrical needs of its customers for an extended period of time. The NERC CIP Standards involve elements such as training, physical and electronic security, systems security management and controls, incident reporting and response, and disaster recovery planning and will have an impact upon employees, supplemental workers, and service vendors who have electronic or physical access to the critical cyber assets and facilities noted herein.

3. CIP Definitions:

   The following definitions shall be used for purposes of these Critical Infrastructure Protection Requirements.

   Certificate of Destruction – certificate annexed hereto (and as it may be amended from time to time) used to confirm that NERC CIP Confidential Information has been disposed of as set forth in this Agreement.

   Critical Assets – (CA) – Select facilities, systems, and equipment, which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of Edison’s Bulk Power System.

   Critical Cyber Assets – (CCA) – Cyber Assets essential to the reliable operation of Critical Assets. This includes, but is not limited to, Cyber Assets operated by, and included in, energy management systems, plant control systems, substation automation, and load shedding.

   Cyber Assets – Programmable electronic devices and communication networks including hardware, software, and data.

   Cyber Security Incident – Any malicious act or suspicious event that: (a) compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or (b) disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.

   Edison’s Bulk Power System – Select Edison-owned assets consisting of grid facilities, electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, which Edison determines are subject to NERC CIP standards.
Electronic Security Perimeter (ESP) – The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.

NERC CIP Access – Authorized cyber access, or authorized Unescorted Physical Access, to a NERC CIP Cyber Asset.

NERC CIP Cyber Assets – Any Cyber Assets to which some or all of the NERC CIP Standards apply, including without limitation: Cyber Assets used in the access control and or monitoring of an Electronic Security Perimeter, and/or a Physical Security Perimeter; other Cyber Assets within identified Electronic Security Perimeters; and Critical Cyber Assets.

NERC CIP Confidential Information – information that Edison, or a governmental agency of competent jurisdiction, has determined relates to Edison’s Critical Assets, Critical Cyber Assets, Electronic Security Perimeter, Physical Security Perimeter, or Edison’s Bulk Power System as those terms are defined in the NERC CIP Standards, and which must be protected pursuant to those Standards. This includes, but is not limited to, operational procedures, lists as required by NERC CIP Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

Non-Disclosure Certificate – certificate annexed hereto by which those who have been granted access to NERC CIP CONFIDENTIAL INFORMATION shall certify their understanding that such access to NERC CIP CONFIDENTIAL INFORMATION is provided pursuant to the terms and restrictions of this Agreement, and that they have read this Agreement and will be bound by its terms.=

Notes of NERC CIP Confidential Information – memoranda, analyses, reports, studies, handwritten notes, or any other form of work-product or information in physical or electronic form which copies or discloses NERC CIP CONFIDENTIAL INFORMATION. Notes of NERC CIP CONFIDENTIAL INFORMATION are subject to the same restrictions as for NERC CIP CONFIDENTIAL INFORMATION except as specifically provided in this Agreement. Unless otherwise instructed by Edison, Contractor shall mark, or otherwise identify, Notes of NERC CIP Confidential Information created by Contractor as NERC CIP CONFIDENTIAL INFORMATION.

Personnel Risk Assessment (PRA) – A background check of an individual that consists of, at a minimum, an examination for criminal convictions and a social security number trace, as well as any other reviews deemed necessary by Edison’s Corporate Security Investigative Support Services division (CSISS) in order to grant NERC CIP Access to that individual.

Physical Security Perimeter (PSP) – The physical, completely enclosed “six-wall” border surrounding computer rooms, telecommunications rooms, operations centers, and other locations in which Critical Cyber Assets are housed and for which access is controlled.

Reviewing Representative – a person who has signed a Non-Disclosure Certificate and who is: (i) an employee or other representative of Contractor who needs access to the NERC CIP Confidential Information to provide goods or services for Edison; or, (ii) a consultant or an employee of a consultant retained by Contractor and needs access to the NERC CIP Confidential Agreement to assist Contractor provide goods or services for Edison.

Significant Changes – The implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware, to a NERC CIP Cyber Asset.

Unescorted Physical Access – Physical access to or within a Physical Security Perimeter without continual, uninterrupted physical escort by approved Edison personnel.

4. Compliance by Contractor:

In connection with its performance under the Agreement, Contractor will comply, and will cause its, and its Subcontractors', employees, agents and representatives to comply, with the provisions of these Critical Infrastructure Protection Requirements. If Contractor fails to comply with the provisions of these Critical Infrastructure Protection Requirements, Edison shall have the right to terminate the Agreement pursuant to the Term and Termination section of the Terms and Conditions (Section 15 in the
5. **NERC CIP Access Requirements:**

5.1 **Compliance with Access Requirements.** Contractor shall identify its, and its Subcontractors’, employees, agents and representatives who will have or require NERC CIP Access in connection with performance of the Services. Edison may, in its discretion, provide such access. If such access is given, Contractor shall provide Edison an updated written list of personnel requiring NERC CIP Access on a quarterly basis, or upon request by Edison. Contractor shall be liable for and reimburse Edison for any costs and expenses incurred due to any breach of this Section 5 of this Exhibit.

5.2 **Consent to Personnel Risk Assessment:**

5.2.1 **Personnel Risk Assessment.** Contractor will allow CSISS (Phone 626-302-7875, FAX 626-302-7881) to perform a PRA on all its and its Subcontractors’ employees, agents and representatives, at Edison’s sole discretion, prior to Edison granting NERC CIP Access or physical or electronic access to other systems or areas deemed appropriate by Edison in connection with the security of a PSP or ESP. A PRA may be conducted by Edison at any time, and Edison reserves the right to change the requirements of the PRA at its discretion. Contractor understands and agrees that CSISS will communicate PRA findings to Contractor and the Edison Representative.

5.2.2 **Non-routine Limited Access.** When the Services requires non-routine limited access to a PSP, Edison at its option may escort Contractor’s and Subcontractors’ employees, agents or representatives onto the Edison location identified as a PSP or CCA, and Contractor’s or Subcontractors’ personnel will be required to remain with the provided Edison escort throughout the term of the access. In such cases, a PRA will not be required.

5.3 **Reassignment or Termination of Contractor Personnel.** When a Contractor or Subcontractor employee, agent or representative with NERC CIP Access is reassigned to non-Edison work, or is no longer employed by Contractor or Subcontractor, Contractor shall immediately verbally notify Edison if such employee, agent or representative was terminated for cause, and notify Edison within 24 hours if the employee, agent or representative was reassigned for any other reason. Upon receipt of notification, Edison may immediately revoke that person’s NERC CIP Access. Unless otherwise agreed by Edison, Contractor shall immediately either (a) deliver to Edison all NERC CIP Confidential Information in the possession or control of such employee, agent or representative, or (b) destroy or render non-readable that NERC CIP Confidential Information, provided Contractor certifies to Edison, in writing, that the NERC CIP Confidential Information was in fact destroyed or rendered non-readable.

6. **NERC CIP Confidential Information:**

6.1 **NERC CIP Confidential Information shall be made available under the terms of this Agreement only to Contractor and only through its Reviewing Representatives as provided in Paragraphs 6.5-6.7 of this Exhibit.** However, if Contractor has previously executed a NERC CIP Nondisclosure Agreement with Edison relating to the work addressed by this Agreement, persons deemed Reviewing Representatives under the Nondisclosure Agreement shall be deemed Reviewing Representatives under this Agreement, and shall not be required to execute individual NERC CIP Nondisclosure Certificates. Individual NERC CIP Nondisclosure Agreements executed pursuant to a NERC CIP Nondisclosure Agreement are adopted by reference within.

6.2 **If Contractor is legally compelled to disclose NERC CIP CONFIDENTIAL INFORMATION,** Contractor will provide Edison with prompt notice so that Edison may seek a protective order or other appropriate remedy – with Contractor’s reasonable cooperation, if requested by Edison. If a protective order or other remedy is not obtained, then Contractor will disclose only that portion of the NERC CIP CONFIDENTIAL INFORMATION that it is legally compelled to disclose and will exercise reasonable efforts to obtain assurance that NERC CIP CONFIDENTIAL INFORMATION will be treated as confidential.

6.3 **If requested by Edison, Contractor shall, within fifteen (15) days,** either:
6.4 All electronic NERC CIP CONFIDENTIAL INFORMATION shall be maintained by Contractor in password-protected or encrypted systems. All physical NERC CIP CONFIDENTIAL INFORMATION shall be maintained by Contractor in secured locations and locked away when not in use. Access to those materials shall be limited to those Reviewing Representatives specifically authorized pursuant to Paragraphs 6.6 and 6.7 of this Exhibit.

6.5 NERC CIP CONFIDENTIAL INFORMATION shall be treated as confidential by Contractor and by the Reviewing Representative in accordance with the certificate executed pursuant to Paragraph 6.7 of this Exhibit. NERC CIP CONFIDENTIAL INFORMATION shall not be used except to provide Services pursuant to the Agreement, nor shall it be disclosed in any manner to any person except a Reviewing Representative who needs to know the information in order to carry out the Reviewing Representative’s responsibilities.

6.6 In the event that Contractor wishes to designate as a Reviewing Representative a person not described in Paragraph 3 above in this Exhibit, Contractor shall seek agreement from Edison. That person shall be a Reviewing Representative pursuant to Paragraph 3 above in this Exhibit with respect to those materials, if an agreement is reached.

6.7 A Reviewing Representative shall not be permitted to inspect, participate in discussions regarding, or otherwise be permitted access to NERC CIP CONFIDENTIAL INFORMATION pursuant to this Agreement unless that Reviewing Representative has first executed a Non-Disclosure Certificate. A copy of each Non-Disclosure Certificate shall be provided to counsel for Edison, or to other duly authorized Edison personnel, before disclosure of any NERC CIP CONFIDENTIAL INFORMATION to that Reviewing Representative.

6.8 Any Reviewing Representative may disclose NERC CIP CONFIDENTIAL INFORMATION to any other Reviewing Representative as long as the disclosing Reviewing Representative and the receiving Reviewing Representative have both executed a Non-Disclosure Certificate, and a copy of each Certificate has been delivered to Edison prior to any such disclosure. In the event that any Reviewing Representative to whom the NERC CIP CONFIDENTIAL INFORMATION is disclosed ceases to qualify as a Reviewing Representative, or is employed or retained for a position whose occupant is not qualified to be a Reviewing Representative under Paragraph 3 of this Exhibit, access to NERC CIP CONFIDENTIAL INFORMATION by that person shall be terminated and Contractor shall be responsible for collecting or destroying all NERC CIP CONFIDENTIAL INFORMATION from the former Reviewing Representative. Every person who has executed a Non-Disclosure Certificate shall continue to be bound by the provisions of this Agreement and the Non-Disclosure Certificate. Upon request by Edison, Contractor shall provide Edison with a list of current Reviewing Representatives.

6.9 All copies of all documents reflecting NERC CIP CONFIDENTIAL INFORMATION created by Contractor, as well as Notes of NERC CIP CONFIDENTIAL INFORMATION, shall be marked “PROTECTED MATERIALS – Contains NERC CIP CONFIDENTIAL INFORMATION,” or shall be marked with words of similar import, as long as the term “NERC CIP CONFIDENTIAL INFORMATION” is included in that designation, to indicate that they are NERC CIP CONFIDENTIAL INFORMATION.

6.10 Contractor and Edison agree that the NERC CIP CONFIDENTIAL INFORMATION provided to Contractor pursuant to this Agreement is exempt from production under the California Public Records Act, California Government Code Sections 6250, et seq., under either the exemption provided in Section 6254(e) or 6255(a), or both, and Contractor agrees to withhold production of such materials unless ordered to do so by a court of competent jurisdiction as provided for in Paragraph 6.2 of this Exhibit.

6.11 In the event that a Reviewing Representative no longer requires access to NERC CIP CONFIDENTIAL INFORMATION, Contractor shall immediately revoke that Reviewing Representative’s access to NERC CIP Confidential Information. Contractor shall also immediately inform Edison that the
Reviewing Representative in question no longer requires access to such information. Edison, however, may extend the time for such notification.

6.12 Termination of Agreement. Notwithstanding anything to the contrary contained in the Terms and Conditions, upon the termination of the Agreement for any reason, Contractor shall, within fifteen (15) days, either: (a) deliver to Edison all NERC CIP Confidential Information in the possession of Contractor, Subcontractors, or any of their respective employees, agents, or representatives, or (b) destroy or render non-readable all the NERC CIP Confidential Information; provided Contractor certifies to Edison, using the attached Certificate of Destruction, that the NERC CIP Confidential Information was in fact destroyed or rendered non-readable. Notwithstanding anything to the contrary contained in the Terms and Conditions, the Contractor shall not be entitled to keep any copy of the NERC CIP Confidential Information in its archives. The return or destruction of the NERC CIP Confidential Information shall not release the Contractor from its obligations under the Mutual Nondisclosure section of the Terms and Conditions (Section 7 in the Terms and Conditions for Services and Related Materials and the Terms and Conditions for Consulting Services, and Section 8 in the Terms and Conditions for Materials and Related Services).

7. NERC CIP Training:

Contractor’s and Subcontractors’ employees, agents and representatives shall complete all NERC CIP training required by Edison prior to being granted Unescorted Physical Access to a PSP or electronic access to an ESP. Further, Contractor shall provide documentation of successful completion of Edison-required annual training on the NERC CIP Standards.

8. NERC CIP Reporting:

8.1 Cyber Security Incident: Contractor shall report any Edison-related Cyber Security Incident to the IT Operations Center (949-587-5534) immediately upon discovery of the incident. Contractor’s report shall include the specific details of the matter, individuals involved, and steps taken in response to that incident. Each specific incident may require additional information from the Contractor, depending upon the underlying facts and circumstances of the incident, which shall be provided to Edison upon request.

8.2 NERC CIP Access Verification: Upon Edison’s request, Contractor shall provide a written report to the Edison Representative with a list of all Contractor and Subcontractor employees, agents and representatives that have NERC CIP Access, or will have a need for NERC CIP Access.

9. NERC CIP Indemnity:

In addition to any indemnity obligations set forth in the Terms and Conditions, Contractor is also responsible for any breach of these Critical Infrastructure Protection Requirements by its or its Subcontractors’ employees, agents or representatives. Contractor shall defend, indemnify and hold harmless Edison, its officers, agents, representatives, employees, assigns, and successors in interest, from and against any and all liability, damages, losses, claims, demands, actions, fines, penalties, assessments, causes of action, costs, (including attorney’s fees and expenses and all costs or expenses related to increased regulatory or administrative oversight), or any of them, arising out of or relating to the breach of these Critical Infrastructure Protection Requirements by Contractor or its Subcontractors, or any of their respective employees, agents or representatives.

10. Contractor-Provided NERC CIP Cyber Assets or NERC CIP Compliance Services:

10.1 Provision of Assets and Significant Changes. If Contractor provides any NERC CIP Cyber Assets (identified as such to Contractor by Edison) to Edison under the Agreement or makes any Significant Changes to existing Edison NERC CIP Cyber Assets (identified as such to Contractor by Edison), Contractor shall ensure that the NERC CIP Cyber Assets and Significant Changes meet the additional requirements of this Section 10.1 of this Exhibit.

10.1.1 All NERC CIP Cyber Assets provided by Contractor or modified by Contractor with Significant Changes that are provided by Contractor must not adversely affect Edison’s existing cyber security controls.
10.1.2 All NERC CIP Cyber Assets and Significant Changes to NERC CIP Cyber Assets that are provided by Contractor shall comply with Edison’s configuration requirements and will only have those ports enabled that are required for normal and emergency operation. Contractor agrees that all other ports and services will be properly disabled prior to use in Edison’s production environment. Contractor must provide a detailed list of all ports and services required by the NERC CIP Cyber Assets for normal and emergency operations.

10.1.3 All NERC CIP Cyber Assets provided by Contractor must either utilize, or support the utilization of, anti-virus software and other malicious software (malware) prevention tools to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware. Anti-virus software utilized or supported must meet or exceed Edison’s anti-virus requirements.

10.1.4 All NERC CIP Cyber Assets provided by Contractor must contain authentication and role based security access that can prevent and detect unauthorized access to Edison’s computing network.

10.1.5 All NERC CIP Cyber Assets provided by Contractor must have the capability to generate and retain logs of sufficient detail to create historical audit trails of individual user account access activity and events related to Cyber Security.

10.1.6 All NERC CIP Cyber Assets provided by Contractor must minimize the use of administrator, shared, and other generic account privileges including factory default accounts. Upon installation of all NERC CIP Cyber Assets, there shall be no capability for shared user access unless agreed to in writing by Edison. Contractor must remove, disable or rename any factory default account prior to the NERC CIP Cyber Asset being placed into use by Edison. If such accounts remain enabled by Contractor during stabilization and testing, passwords must be changed prior to Contractor transferring any NERC CIP Cyber Asset into service in a production environment.

10.1.7 All NERC CIP Cyber Assets provided by Contractor must enforce the use of complex passwords, containing at least six characters, and must include a combination of letters, numbers, and special characters. If Edison requires two factor authentication or biometrics, Contractor must also comply with this requirement as noted in Edison’s policy.

10.1.8 Any Significant Changes made or implemented by Contractor must not cause Edison NERC CIP Assets to become noncompliant with this Section 10.1 of this Exhibit.

10.2 Provision of Services. If Contractor is engaged to perform a service for Edison relating to Edison’s compliance with the NERC CIP Standards, including without limitation, activities such as cyber security vulnerability assessment, procedure documentation, remediation activities, system testing, maintenance, and configuration documentation, Contractor shall ensure that its activities meet the additional requirements of this Section 10.2 of this Exhibit.

10.2.1 Contractor’s activities must not adversely affect Edison’s cyber security controls.

10.2.2 If Contractor performs testing of any NERC CIP Cyber Assets, Contractor shall ensure that its activities meet the following requirements.

10.2.2.1 Contractor must conduct its testing in a manner that minimizes adverse effects on Edison’s production system and its operation.

10.2.2.2 Contractor shall document in writing upon the completion of the system testing that Contractor’s testing has been performed in a manner that reflects Edison’s production environment, and will also provide Contractor’s test plan and the results of the testing.

10.2.2.3 Contractor shall consult with Edison on the scheduling and conduct of all tests performed pursuant to Edison’s requirements and policies.

10.2.3 If Contractor provides support or maintenance for Edison NERC CIP Cyber Assets, Contractor shall grant Edison access and rights to configure the assets in accordance with Edison’s requirements.
10.3 Enhancements to NERC CIP Cyber Assets Pursuant to Agreement. If Contractor has a continuing obligation under the Agreement to provide software or firmware updates, upgrades, patches, new versions or other enhancements, including Significant Changes, to any NERC CIP Cyber Assets (identified to Contractor as such by Edison) to Edison, Contractor must meet the additional requirements of this Section 10.3 of this Exhibit:

10.3.1 Contractor must notify Edison of the availability of software security patches and upgrades for such NERC CIP Cyber Assets. The notification must be made to Edison in writing within 15 calendar days of the availability of the security related patches or upgrades.

10.3.2 If Contractor provides any third party software in conjunction with Contractor’s own product, (i) Contractor shall notify Edison of security patches and upgrades pertaining to such other third party software. Such notification shall be made in writing within 15 calendar days of availability of the security related patches or upgrades.

11. NERC CIP Right to Audit.

Contractor will maintain records of compliance by itself and all Subcontractors, agents and Representatives, the terms of this Agreement for three (3) years after the completion of this Agreement. Edison reserves the right to audit and copy any applicable documents related hereto. Edison shall, at its discretion, assign the audit and duplication rights of this paragraph to a governmental agency or entity operating under the authority of a governmental agency.
ATTACHED CERTIFICATES
CONTRACTOR NERC CIP
NON-DISCLOSURE CERTIFICATE

I hereby certify my understanding that access to SCE NERC CIP CONFIDENTIAL INFORMATION is being provided to me pursuant to an agreement ("Agreement") entered between Southern California Edison Company and Contractor, that I have been given a copy of and have read the Agreement, and that I agree to be bound by its terms.

I understand that the contents of NERC CIP CONFIDENTIAL INFORMATION, any notes or other memoranda, or any other form of information that copies or discloses such information, shall not be disclosed to anyone other than in accordance with the Agreement. I shall return or destroy all NERC CIP CONFIDENTIAL INFORMATION and Notes of NERC CIP Confidential Information in my possession, custody or control to SCE or Contractor when I no longer have any need for such information.

This information was provided to me at the request of:

Contractor: ______________________________

Signed: ________________________________

Print full name: __________________________

Title: _________________________________

Phone Number: _________________________

Date: _________________________________

My Employer: __________________________
GENERAL NERC CIP  
CERTIFICATE OF DESTRUCTION

I am an officer of the Company listed below. My Company was previously given access to NERC CIP Confidential Information.

This Certificate addresses the following type of NERC CIP Confidential Information:

Circle One:

1. Any of Edison’s NERC CIP Confidential Information.

2. Edison’s NERC CIP Confidential Information relating to: (insert Purchase Order number or RFP number, i.e. “PO 1234”): ____________________________

I certify that I have instructed my employees, subcontractors, and representatives to search for all NERC CIP Confidential Information, and Notes of NERC CIP Confidential Information, in their possession, custody, or control. I also instructed them to either send to me (or my authorized representative) all such information, or to destroy or erase that information. Based on the results of that search and my instructions, I also certify that, to the best of my knowledge, no one in my organization, either past or present, currently possess and of Edison’s NERC CIP Confidential Information in any form.

Name of Company: _______________________________________________________

If Company was a subcontractor, then include name of General Contractor/Primary Employer:

_____________________________________________________________________

Executed on the following date: _______________, by:

_________________________________________________
Signature

_________________________________________________
Name

_________________________________________________
Position