EXHIBIT [ ]

INFORMATION SECURITY, CYBERSECURITY, AND PRIVACY REQUIREMENTS FOR SUPPLIERS[1]

This Exhibit ("Cyber Requirements Exhibit") provides the cybersecurity and privacy requirements Supplier must maintain as long as Supplier has access to Edison's Computing Systems or access to, possession, custody, or control of Edison Data. These procedures are in addition to the security and confidentiality requirements of the Agreement and present a minimum standard only.

It is Supplier's obligation to (i) implement and maintain appropriate measures to protect its electronic network and systems from Cyber Incidents that could make Edison's Computing Systems vulnerable to unauthorized access or use and to protect Edison Data in its possession, custody, or control from accidental or unauthorized access, acquisition, disclosure, use, modification, loss, damage, or destruction; (ii) regularly review and revise those measures to address new or ongoing risks and to implement industry best practices and legal requirements regarding cybersecurity and privacy; and (iii) to cooperate with Edison in its efforts to minimize risks to Edison's Computing Systems and Edison Data and reduce the impact of any unauthorized access to the Edison's Computing Systems, or disclosure or unauthorized use of Edison Data.

Supplier's security measures to protect its electronic network and systems from Cyber Incidents that could make Edison's Computing Systems vulnerable to unauthorized access or use and to protect Edison Data in its possession, custody, or control shall be no less rigorous than industry cybersecurity and privacy best practices. Without in any way limiting the generality of the foregoing, Supplier's security and privacy practices and procedures must address the following areas and comply with the requirements in the sections that follow. Certain provisions specifically relating to access to Edison's Computing Systems or to CEII, EPI, BES Cyber System or BES Cyber System Information are not applicable if Supplier does not have access to Edison's Computing Systems or to CEII, EPI, BES Cyber System or BES Cyber System Information. Those provision will only become applicable when Supplier is given access to Edison's Computing System or to CEII, EPI, BES Cyber System or BES Cyber System Information.

A. Management of Information Security

Supplier shall maintain, update as necessary, and adhere to a comprehensive written information security program (the "Information Security Program") that: (i) contains appropriate administrative, technical, and physical safeguards to protect its electronic network and systems from Cyber Incidents that could make Edison's Computing Systems vulnerable to unauthorized access or use and to protect Edison Data in its possession, custody, or control; (ii) complies with applicable laws and regulations and conforms to industry best practices; (iii) is reviewed and revised for adequacy and effectiveness at regular intervals (at least annually and whenever there is a change in Supplier's practices that may affect the security of Edison Data or Edison's Computing Systems). While providing the Services, Supplier shall not alter or modify its Information Security Program in such a way that it will weaken or compromise the confidentiality, availability, or integrity of Edison Data or Edison's Computing Systems.

[1] As used herein, Supplier means the party to the Agreement that provides services or products to Edison, which party may be referred to in the Agreement as, without limitation, Contractor, Consultant or Licensor.

B. Employee Policies

1. Security and Privacy Awareness and Training

Supplier shall provide its personnel with privacy and information security training before providing such personnel access to Edison's Computing Systems or Edison Data and at least annually thereafter. Additionally, Supplier shall use written acceptance of codes of conduct, ethics policies, or confidentiality agreements, to promote employee awareness and compliance with Supplier's information security and privacy policies and procedures. Supplier shall maintain employee completion reports and make such completion reports available to Edison upon Edison's written request. Supplier shall review the contents of its security and privacy awareness and training program at least annually to ensure it is updated and reflects current, relevant security information.

Depending upon the nature of the engagement Edison may specify in the purchase order, work order, or statement of work that Supplier shall supplement its information security training program with training or materials that Edison provides.

Supplier shall require that its internal and third-party software developers remain current on application security and secure coding best practices and that they regularly attend formal application security training programs.

Upon request, Supplier shall certify compliance with these training requirements.

2. Background Investigation

In accordance with industry best practices and applicable laws, Supplier shall conduct a background investigation for every employee receiving access to Edison's Computing Systems or Edison Data. For new hires and current employees who do not yet have access to Edison's Computing Systems or Edison Data, the background check shall occur before the employee receives such access. For existing employees who already have access to Edison's Computing Systems or Edison Data, the background check should be conducted promptly. Background checks must include the following:

a. Background verification including whether the prospective employee has been convicted of a felony, property crime or fraud in any state where the individual has resided, studied or worked during the past seven years; and

b. Check of United States' Specially Designated Nationals List and the Denied Persons List.

C. Supplier/Service Provider Management

Supplier shall assess and track cybersecurity and privacy risk associated with Subcontractors or its service providers with access to Edison's Computing Systems or Edison Data and shall take all commercially reasonable actions to promptly remediate these risks. Supplier shall contractually obligate Subcontractors or its service providers to (1) use industry best practices to protect their electronic network and systems from Cyber Incidents that could make Edison's Computing Systems vulnerable to unauthorized access or use and to protect Edison Data when accessed, processed, or stored by a Subcontractor or service provider and (2) immediately report to Supplier any reasonably suspected or confirmed Cyber Incident that could impact Edison's Computing Systems or Edison Data.

D. Off-Shoring

Supplier shall not permit access to Edison's Computing Systems or transmit, access, use, or store Edison Data outside the United States without the prior written permission of Edison's Vice-President for Information Technology or the Director of Cybersecurity. Supplier is responsible for understanding and complying with the applicable cybersecurity and privacy laws and regulations of the foreign jurisdictions from which Edison agrees that Edison's Computing Systems or Edison Data may be accessed, used, or stored. As part of any offshoring request, Supplier shall inform Edison of any applicable foreign laws or regulations that may reduce the confidentiality, availability or integrity of Edison's Computing Systems or of Edison Data or impose additional burdens on Edison.

E. Asset Management

All of Supplier's or its Subcontractor's devices, including cell phones or other portable storage devices, used to store Edison Data shall be equipped with industry standard security and encryption features, which shall include at a minimum remote wipe and remote shutdown capabilities. Supplier's and Subcontractors' personnel may not access or store Edison Data on any personal or third-party devices, including mobile devices, tablets or personally owned laptops, unless such devices have been configured with industry standard security and encryption features, which shall include at a minimum remote wipe and remote shutdown capabilities.

F. Physical and Environmental Security

Supplier shall take appropriate steps to prevent unauthorized physical access, as well as accidental and intentional damage, to Supplier's physical premises and electronic systems that access, use, store or otherwise process Edison's Data. Supplier shall also protect against environmental risks (e.g. earthquakes, tornados, power failures) including by appropriate redundancies and backups) and systems malfunctions or failures.

G. Communications and Operations Management

Supplier shall maintain written procedures and technological controls for the following areas.

1. Network Security - IDS/IPS Use and Signature Updates

Supplier shall subject all network traffic to electronic review and monitoring.

Supplier shall use Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) systems that generate alerts containing enough information to detect and evaluate a potential incident. The IDS/IPS systems shall have the latest signatures applied in order to effectively monitor for the most recent threats and vulnerabilities.

2. Network Security - Firewall(s)

Supplier shall segregate its connected networks and electronic systems to protect them from outside threats. This shall include utilizing industry standard firewalls to segment and protect the organization's internal network from the Internet, and to segregate systems that access, use, or store Edison Data from other less restricted internal networks and systems.

3. Firewall Configuration

On public-facing firewalls, Supplier shall disable all ports and services that are not required for documented business purposes.

4. Network Logging

Supplier shall use industry best practice monitoring and logging technologies to record relevant actions involving access to Edison's Computing Systems or Edison Data.

5. Malware Protection

Supplier shall use anti-malware software on networks, servers, workstations and portable devices that may be used to access Edison's Computing Systems, or to access, use, or store, Edison Data; the malware signatures shall be regularly updated in a timely manner.

6. Patches and Updates

Supplier shall follow industry best practices for patching and updating software and firmware on networks, servers, workstations and portable devices that may be used to access Edison's Computing Systems, or to transmit, access, use, or store, Edison Data.

7. Administrative Activity

Supplier shall minimize administrative privileges and allow personnel to only use administrative accounts when required.

Supplier shall log and monitor network, server and workstation activities, including log-in attempts, to record administrative activity for accountability and audit purposes.

8. Log Monitoring and Retention

Supplier will maintain and review audit logs for anomalies.

Supplier shall retain system and network logs for at least one year after the engagement is completed to allow for the successful auditing of historical events, to meet legal requirements, and for law enforcement and forensic purposes of either Supplier or Edison.

9. Email Relaying

Supplier shall secure access and prevent misuse of its own email resources.

10. Physical Media Tracking

Supplier shall establish effective processes and procedures for handling, storing and transporting media to protect Edison Data from unauthorized access and/or disclosure.

11. Unapproved Wireless Networks

Supplier shall have all network connections and devices adequately tracked, managed, authorized, and controlled to protect against threats and to maintain security for the systems and applications using the network.

12. Wireless Networks Encryption

Supplier shall implement processes and tools to control the use of wireless local area networks, access points and wireless systems, including industry best practice encryption for authorized wireless access points.

13. Network Security- Authorized Network Traffic

Supplier shall formally review, approve, and authorize all permitted network services.

14. System and Data Recovery

Supplier shall regularly back-up Edison Data and systems that access, store or use Edison Data. Backups of these systems and data shall be available, including in the event of a disaster and the ability to restore from such backups shall be tested periodically.

15. Change Control

Changes affecting Edison's Computing Systems or Edison Data must be made within a formal change control program.

16. Data Encryption

a. Edison Data, including any backups, must always be secured through industry best practice whole disk or media encryption and file or database encryption (if applicable) and strong access controls; and

b. Transmission of Edison Data must always be encrypted (using industry best practices).

H. Access Control

Supplier shall control access to its technology assets and Edison Data, including implementation of the following requirements:

1. Password Controls

Password controls must meet industry best practices, including but not limited to:

(i) Encrypting passwords using "hashing" and "salting" techniques, in transit and at rest;
(ii) Enforcing password complexity requirements on users;
(iii) Limiting failed attempts before lockout;
(iv) Prohibiting obvious, common, or reused passwords; and
(v) Not sending credentials through email for password resets.

2. Logical and Physical Access Authorizations and Suspensions

Supplier shall limit access to Edison's Computing Systems and Edison Data only to active users who require access to perform the Services. Supplier shall immediately notify Edison management to promptly revoke or disable user access rights to Edison's Computing Systems and to Edison Data of any employee who is terminated, resigns, or retires, or who is reassigned from work requiring access to Edison's Computing Systems or to Edison Data. Supplier also shall immediately revoke the employee's or former employee's access to Edison Data in Supplier's possession, custody, or control.

3. Multifactor Authentication for Remote Access

Supplier shall use two-factor authentication for remote access to systems that access or store Edison Data.

4. Logging and Monitoring of Persons with Access to BES Cyber System Information

Supplier shall track and monitor Supplier employees, agents, and subcontractors who have access to BES Cyber System Information in Supplier's possession, custody, or control. Supplier shall maintain logs identifying (i) such persons to whom Supplier provides access to BES Cyber System Information in Supplier's possession, custody, or control; (ii) whether such persons have been trained or re-trained, if training is required by Edison; and (iii) the dates that Supplier provided or revoked that person's access rights to BES Cyber System Information. Supplier shall provide this information upon request by Edison.

5. Return or Destruction of Edison Data

As between Edison and Supplier, all Edison Data shall be and remain the property of Edison. Unless different requirements regarding the retention and destruction of Edison Data are included in the "Confidentiality" or "Non-Disclosure" section of the Agreement, the following requirements shall apply to all Edison Data: At the end of each engagement, Supplier may keep one copy of the Edison Data solely for back-up storage purposes, except that all BES Cyber System Information must be rendered irretrievable as soon as possible, but in no event more than fifteen (15) days after the conclusion of the engagement, regardless of how it is stored or accessed. Within fifteen (15) days after the conclusion of the engagement, Supplier shall provide Edison with a written confirmation executed by a manager or officer of Supplier confirming that all BES Cyber System Information in its possession, custody or control has been rendered irretrievable. The destruction of all Edison Data shall require use of industry best practices for rendering information irretrievable.

I. Security Incident and Communications Management

Supplier shall implement a formalized information security incident management program (the "Security Incident Management Program"). The program shall describe how the organization will report incidents internally and to affected external parties. It shall also identify Supplier's incident response team (the "Supplier Incident Response Team") and define their roles and responsibilities.

1. Technical Compliance Checking – Vulnerability Testing and Remediation

Supplier shall regularly scan systems for vulnerabilities. Supplier shall rank all vulnerabilities and promptly remediate detected vulnerabilities ranked as critical, high or moderate. Supplier will use commercially reasonable efforts to identify and notify Edison in writing within one business day of identification of any critical, high or moderate vulnerabilities, risks or threats that could potentially impact Edison Data and that Supplier cannot remediate within 30 days. If Supplier later determines that it cannot remediate within 30 days, it shall promptly notify Edison via email to cybersecurity@sce.com. Supplier's notification shall provide detailed information describing the controls used to mitigate these un-remediated vulnerabilities, risks, or threats.

2. Information Security Incident Management Policy & Procedures Content

Supplier shall establish, document and distribute a formal Security Incident Management

Program, which includes the reporting procedure for a Cyber Incident involving Supplier or any Subcontractor or service provider, the requirement of a Supplier Incident Response Team, escalation procedures, and remediation process, and which provides for periodic testing. Any reasonably suspected or confirmed Cyber Incident must be reported to Edison via email to cybersecurity@sce.com immediately for any Cyber Incident relating to a NERC CIP Project or BES Cyber System Information, CEII, or EPI and as soon as possible but in no event more than one business day after Supplier's awareness of any other Cyber Incidents or as sooner required by Applicable Laws. Notification shall include the nature of the event, date and time of the event, suspected amount of information and type of information (e.g., EPI, NERC CIP) exposed and steps being taken to investigate the circumstances of the exposure. Supplier will take all necessary steps to eliminate or contain the Cyber Incident and Supplier must cooperate with and assist Edison's Cybersecurity Incident Response Team in the investigation, analysis and resolution of Cyber Incidents, including if requested by Edison, providing breach notifications to individuals and regulatory and law enforcement agencies or providing support to Edison if Edison decides to send out such notices. Supplier shall provide Edison with details of the investigation and final disposition of the Cyber Incident relevant to the services provided to Edison or which may impact the confidentiality, integrity, or availability of those services.

J. Subpoenas for Edison Data

Unless prohibited by law or court order, Supplier shall, within five (5) business days of receipt of a subpoena for disclosure of any Edison Data, provide written notice to Edison pursuant to the notices section of the Agreement so that Edison and Supplier may engage in good faith discussions about the appropriate response to the subpoena. If Edison informs Supplier that it will seek to quash or modify the subpoena, then Supplier shall delay responding to the subpoena to permit Edison time to quash or modify the subpoena. If requested by Edison, Supplier shall within fifteen business days of receiving the request confirm whether it received any subpoena for Edison Data within the prior twelve months and the date and scope of all such subpoenas. Nothing in this Cyber Requirements Exhibit is intended to preclude Supplier from complying with the subpoena when and as required to do so by law or court order.

K. Changes in Law

If either Supplier or Edison becomes aware of any changes to the law related to the subject matter of this Cyber Requirements Exhibit, then that Party shall notify the other Party of the change, and the Parties shall meet in good faith as soon as practicable to discuss achieving compliance with the changed legal requirements.

L. Additional Security-Related Requirements For Materials and Products Provided by Supplier

1. Ongoing Vulnerability Assessments, Notification & Patching

If Supplier provides materials or physical goods under this Agreement, Supplier shall regularly assess such materials or goods (including third party or open source software, firmware and hardware) for cybersecurity-related vulnerabilities, risks or threats or defects ("Vulnerabilities"). Supplier shall rank all such Vulnerabilities and promptly remediate any such Vulnerabilities ranked as critical, high or moderate. Supplier will use commercially reasonable efforts to identify and notify Edison in writing within one (1) business day of identification of any such critical, high or moderate Vulnerabilities. Such notification shall be made to cybersecurity@sce.com. Supplier shall promptly send Edison any patches or other technical remediations developed by Supplier to address those Vulnerabilities within thirty (30) days after discovering the Vulnerability.

If Supplier determines that it cannot remediate the Vulnerability within the timeframe specified above, Supplier shall promptly notify Edison via email to cybersecurity@sce.com that remediation is not available. Supplier's notification shall provide detailed information describing recommended controls to mitigate un-remediated Vulnerabilities.

Where third-party hardware, software (including open-source software) and firmware is provided by Supplier to Edison under this Agreement, Supplier shall provide appropriate hardware, software and firmware updates to remediate Vulnerabilities or weaknesses within thirty (30) calendar days after discovery thereof.

2. Confirmation of Secure Delivery and Product or Material Authenticity

Supplier shall establish, document, and implement, a risk management plan to securely deliver hardware, software (including patches), and firmware (including patches) to Edison. Such plan shall conform to industry best practices.

Within fifteen (15) calendar days of a request made by Edison, Supplier shall provide documentation to Edison demonstrating the integrity and authenticity of software, firmware, hardware and firmware provided by Supplier to Edison. This documentation may include (but is not limited to) documentation regarding Supplier's: chain of custody practices, inventory management program (including the location and protection of spare parts); patch management processes; confirmation that Supplier has implemented appropriate updates and patches to third-party hardware, software, firmware and services for software provided to Edison under this Agreement.