Southern California Edison

Customer-Owned Telemetry Procedures

Version: October 22, 2025

Southern California Edison
2244 Walnut Grove Avenue
Rosemead, CA 91770

Table of Contents

- End of Table of Contents -

REVISION NOTES

Date	Notes / Revisions
August 11, 2025	New SCE's Customer-Owned Telemetry Procedures filed with Advice 5612-E.
October 22, 2025	Updated Customer-Owned Telemetry Procedures correcting typographical errors.

List of Acronyms:

Acronyms and Abbreviations	
BESS	Battery Energy Storage System
COT	Customer-Owned Telemetry
CPUC	California Public Utilities Commission
CSIP	Common Smart Inverter Profile
DER	Distributed Energy Resources
DERMS	Distributed Energy Resources Management System
GW	Gateway
IC	Interconnection Customer
IEEE	Institute of Electrical and Electronics Engineers
MS	Millisecond
MVA	Megavolt Ampere
OS	Operating System
PCC	Point of Common Coupling
PTO	Permission to Operate
PV	Photovoltaics
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
SCE	Southern California Edison
URL	Uniform Resource Locator
VAR	Volt-ampere Reactive (Reactive Power)
W	Watt

Customer-Owned Telemetry (COT) Procedures

1 Introduction

1.1 Summary

Consistent with the California Public Utilities Commission (CPUC) Resolution E-5038[1], Southern California Edison (SCE) is implementing an Institute of Electrical and Electronics Engineers (IEEE) 2030.5 telemetry program using customer-owned and managed gateways (GWs) or contracted aggregators[2] (referred to herein as Customer-Owned Telemetry (COT)). SCE's Distributed Energy Resource Management System (DERMS) uses the Common Smart Inverter Profile (CSIP) of IEEE 2030.5 protocol as specified in Rule 21 to communicate with customer generating facility's COT.

1.2 Purpose of These Procedures

Per Resolution E-5038 Ordering Paragraph 2, this document provides "specific technical requirements for telemetering of distribution-connected systems 1 MW or greater and less than 10 MW"[3]. This document also describes the specifications, tests, and approvals of IEEE 2030.5/CSIP GWs and aggregator's ability to conform to telemetry requirements and to interoperate with SCE's DERMS.

1.3 COT Scope

The COT acts as a protocol translation device and aggregation system for the site Distributed Energy Resource (DER) metering. Per Resolution E-5038 Ordering Paragraph 2, interconnection customers (ICs) may use either cellular modem or customer-provided dedicated internet connection to communicate telemetry data back to the COT aggregator or SCE's DERMS. The GW or aggregator provider or the IC's installer is required to integrate the GW or aggregator with the DER systems (DERs or DER meters).

2 SCE COT Process

When SCE makes the determination that telemetry for a generating facility is required (in accordance with Rule 21, Section J.5), and the IC chooses IEEE 2030.5 COT, then the IC is responsible for ensuring that the processes and requirements contained in this document are adhered to prior to completing the interconnection and receiving Permission to Operate (PTO) from SCE.

If the generating facility requires telemetry and the IC selects COT as their desired telemetry option, the following process will apply:

- The IC chooses a COT vendor and type from the SCE's Approved COT GWs and Aggregators list (refer to Section 11 below).

[1] https://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M401/K369/401369674.PDF

[2] The term "aggregator" aligns with the use of the term in CSIP and refers to a cloud-based CSIP Aggregator EndDevice client.

[3] Resolution E-5038, OP 2, pg. 18.

- In accordance with the applicable interconnection process pursued by the IC, the IC and SCE will negotiate and enter into an Interconnection Agreement that includes the COT telemetry vendor and type chosen by the IC, as well as the configuration and functionality agreed to between SCE and the IC.
- The IC completes the required COT form containing the necessary information required by SCE (which includes the IEEE 2030.5 configuration parameters and relevant DER information).
- The IC works with their selected COT vendors and/or installers to complete telemetry installation, implement and test the appropriate configuration, and support commissioning activities with SCE.
- The IC or their COT vendor/installer schedules DERMS telemetry commissioning with SCE.
- Once DERMS commissioning, testing, and other pending site interconnection work is completed (as required by the Interconnection Agreement), SCE will issue a PTO for the generating facility.

3 Telemetry Requirements

3.1 Metering Configuration

Telemetry sites with multiple DER technology types (e.g., photovoltaics (PV) and battery energy storage systems (BESS)) *shall* provide separate aggregate metering for each technology type as depicted by M1, M2, and M3 in the example shown in Figure 1. Net facility-level metering (normally at the Point of Common Coupling (PCC)), as depicted by M4 in Figure 1, is optional.

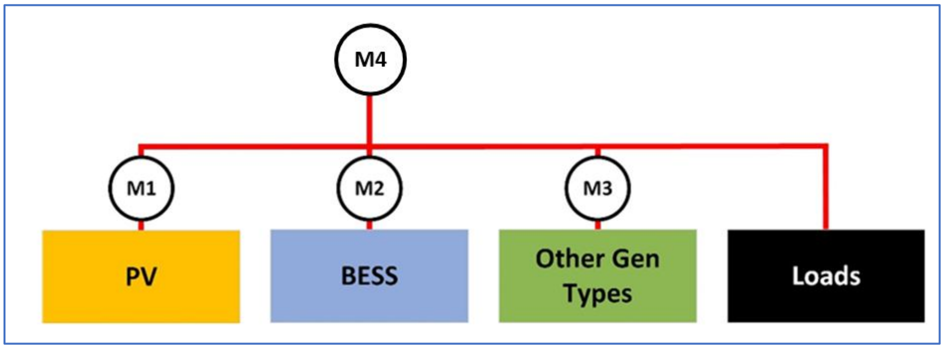

Figure 1- Multi-DER Technology Types Metering

Telemetry sites with one or more generating facilities of a single DER technology type *shall* provide aggregate metering for that DER type as depicted by M1 in Figure 2. Metering at the PCC, as depicted by M2 in Figure 2, is optional.

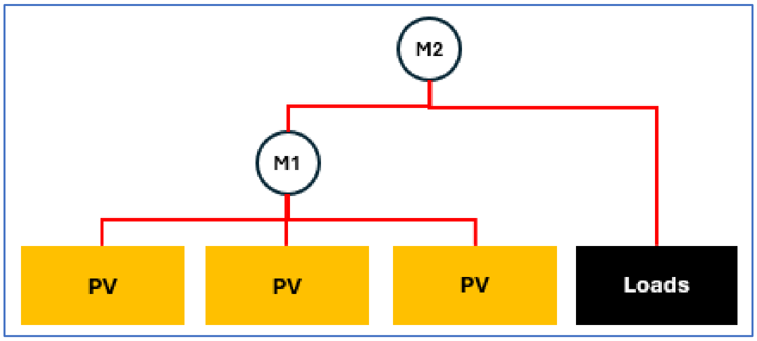

Figure 2 - Single DER Technology Type Metering

3.2 Required Data Points

For each of the technology types existing at the site (as discussed in Section 3.1 above), telemetry *shall* include the following data points:

- Per phase & total 3 phase Watts (W)
- Per phase & total 3 phase volt-amperes-reactive (VAR)
- Per phase voltage (V)
- Frequency (Hz)
- Timestamps representing when the data was recorded/measured

3.3 Sampling Frequency

COT data *shall* be provided to SCE's DERMS at 30 second intervals or less. The DER meter telemetry data *shall* be collected and provided to the COT GW or aggregator at intervals that support the 30 second DERMS posting rate requirements.

4 DER Control Requirements

As deemed applicable, telemetry sites may be required to support the ability to disable permit service based on signals from DERMS. DERMS will use DERControls:opModEnergize for this signal. Requirements are as follows:

a) If opModEnergize=false, COT GWs or aggregators *shall* cease power production from the DER

b) If opModEnergize=true, COT GWs or aggregators *shall* allow for resumption of power production

5 COT Operation and Maintenance Requirements

a) Prior to receiving PTO, DERMS commissioning testing and operational commissioning tests (when required) *shall* be conducted in coordination with SCE.

b) During operation, the IC *shall* ensure the COT and its connection to the DER, metering, and communication equipment is maintained at all times.

c) The IC *shall* ensure the COT connection and data transmission to DERMS is maintained at all times. Upon identifying a COT related malfunction, the IC or their contracted vendor shall make the corresponding repairs as soon as possible. If such repairs cannot be done within 30 days from identifying the malfunction, the IC should notify SCE via email to Rule21@sce.com and include a description of the malfunction along with a repair plan and the expected date of resumption of telemetry.

- Refer to the generating facility's Interconnection Agreement for any operation restrictions that may apply during a period of time when telemetry is not available.
- Security-related patching may be required in a shorter time-frame.

d) If the IC plans to make modifications to the DER, metering or communication equipment that will result in inaccurate data or non-transmission of data to the DERMS, the IC *shall* notify SCE via email to Rule21@sce.com at least 10 business days prior to modifications. The IC *shall* not make modifications without email approval from SCE. The email notification *shall* include:

- Proposed modifications and reasoning
- Expected date of resumption of telemetry
- If necessary, new information that will be needed by SCE to collect COT-provided telemetry

e) After restoration of power to the telemetry site, COTs *shall* immediately poll for new DER controls to follow (e.g., COT GW must immediately GET DERMS DERControls to ensure that opModEnergize=true prior to re-energization).

f) COT aggregators *shall* ensure DERs comply with DERMS opModEnergize DERControl after an outage at a telemetry (e.g., do not energize if opModEnergize=false)

g) Once re-energization is complete, COT *shall* begin posting data to DERMS as required in this procedure.

h) If COT temporarily loses communications with DERMS for any reason, COT should continue to collect the required data point, as possible. After restoration of communications with DERMS, the COT *shall*:

- Immediately post the readings recorded during the period when communication with DERMS was lost, as available, and resume posting data at specified intervals, and
- Poll for new DERControls.

6 COT Requirements

6.1 COT General Functional Specifications

a) COT GWs and aggregators supporting multi-DER technology type telemetry sites (as described in section 3.1 Figure 1, above) *shall* be tested and certified as a Common Smart Inverter Profile (CSIP)[4] aggregator client (Aggregator Profile).

COT GWs supporting single-DER type telemetry sites (as described in section 3.1 Figure 2, above) *shall* be tested and certified as either (i) a Common Smart Inverter Profile (CSIP) aggregator client (Aggregator EndDevice), or (ii) as a CSIP DER client (DER EndDevice).

[4] https://sunspec.org/2030-5-csip-specifications/ (Current approved version is 2.1)

b) COT GWs and aggregators *shall* be able to be configured to implement the number of DER EndDevices necessary to support the telemetry requirements identified in Section 3.1 (or only one EndDevice for a single-DER type telemetry site).

c) COT GWs and aggregators *shall* be approved by SCE prior to IC use.

d) COT GWs and aggregators *shall* use the Time Function Set to synchronize time with DERMS.

6.2 COT GW DERMS Access Requirements

a) COT GWs *shall* use polling to access DERMS.

b) COT GWs *shall* poll the DERControlList every 30 seconds.

c) COT GW's aggregator EndDevice *shall* poll once per day for updates to its EndDeviceList, Time, and for changes to other resources (except for DERControls – See 6.2.b and Section 5f).

d) After resumption from loss of power or communications with the server, COT *shall* poll for updates immediately and once per day thereafter.

6.3 COT Aggregator DERMS Access Requirements

a) Aggregators *shall* support Subscriptions as defined in CSIP Requirements.

b) Aggregators *shall* renew subscriptions every 24 hours.

c) Aggregators *shall* fall back to polling if notifications are not working per CSIP Requirements.

d) If falling back to polling, aggregators *shall* poll the DERControlList every 30 seconds

e) Exception: After an outage at the telemetry site the aggregator shall poll for new DERControls immediately–see also Sections 5(e) and 5(f), above.

f) For all other resources (e.g., dcap, tm, etc.), aggregators *shall* limit polling to once at startup (including after power loss) and once per day thereafter.

6.4 Additional Hardware & Software Requirements for COT GW

a) COT GWs *shall* have the following documentation available:

- System Installation Guide
- System Administrator Guide
- User (Operator) Guide
- Functional Specifications and Related Technical Specifications
- System Configuration Hardening Guide

b) COT GWs *shall* have a secure interface to allow IC or IC's vendors to access and manage:

- Software and Firmware updates (including CSIP versions and patches)
- Configuration of DERs/Meters and DER telemetry and data mapping
- Configuration of protocol and network parameters including DERMS endpoint information (e.g., URL, DeviceCapability path, and Port)

- Access to COT GW aggregator EndDevice's LFDI and PIN
- Validation of receipt of DER telemetry data
- Configuration of security parameters including user access and updating certificates

c) COT GWs *shall* be able to translate between CSIP and device SunSpec Modbus or DNP3 protocols. COT GWs *should* support both SunSpec Modbus and DNP3.

d) COT *shall* support DER EndDevices operating without a FunctionSetAssignmentsListLink (i.e., as a telemetry-only resource and not in a DERProgram).

e) COT GWs and aggregators *shall* support mTLS and Server Name Indication (SNI).

f) COT GWs and aggregators *shall* support SCE issued certificates[5] and support the following cipher suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

g) COT GWs *shall* support both serial and IP DER communications.

h) COT GW *shall* be an OS embedded type of device.

i) COT GW *shall* have a minimum operating temperature range: -20° C to +70° C Preferred operating temperature range: -40° C to + 85° C.

j) COT GW (all GW equipment) *shall* be capable of being installed inside an outdoor cabinet.

6.5 Metering Points Requirements for COT GW

a) Each metering point identified in Section 3.1 *shall* be configured as a DER EndDevice on the COT and an associated MeterUsagePoint *shall* be created on DERMS by the COT with required IEEE 2030.5 fields and the following stipulations:

- The MUP description *shall* be provided and include a description field that describes the source(s) of the meter data (e.g., technology type- PV, Storage, etc.)

b) COT *shall* provide the Table 1 data points/IEEE 2030.5 bits to be set for the IEEE 2030.5 ReadingType and Reading parameters with the following stipulations:

- description shall describe the data type from Table 1
- ReadingSets shall not be used

c) MMRs *shall* include a Timestamp (TimeType) indicating when the Reading occurred.

- The timestamp *shall* be either lastUpdateTime or timePeriod where *duration* *shall* be 0 and *start* *shall* be the reading time

[5] SCE uses a public Certificate Authority. SCE issued certs will not conform to IEEE 2030.5 Certificate Extensions.

Table 1- 2030.5 Reading Parameters

Data Type	2030.5 Reading Type & Reading Parameters			Precision	Notes
	Accumulation Behavior	**Phase**	**UOM**		
Active Power A	12	128	38	1 W	Positive= Export to Grid
Active Power B	12	64	38	1 W	Positive= Export to Grid
Active Power C	12	32	38	1 W	Positive= Export to Grid
Total Watts	12	224	38	1 W	Positive= Export to Grid
Reactive Power A	12	128	38	1 VAR	Positive= Capacitive Load
Reactive Power B	12	64	38	1 VAR	Positive= Capacitive Load
Reactive Power C	12	32	38	1 VAR	Positive= Capacitive Load
Total VARs	12	224	63	1 VAR	Positive= Capacitive Load
Voltage AN	12	129	29	0.1 V	Use for Wye connected meter.
					Omit for Delta connected meter.
Voltage BN	12	65	29	0.1 V	Use for Wye connected meter.
					Omit for Delta connected meter.
Voltage CN	12	33	29	0.1 V	Use for Wye connected meter.
					Omit for Delta connected meter.
Voltage AB	12	132	29	0.1 V	Use for Delta connected meter.
					Omit for Wye connected meter.
Voltage BC	12	66	29	0.1 V	Use for Delta connected meter.
					Omit for Wye connected meter.
Voltage CA	12	40	29	0.1 V	Use for Delta connected meter.
					Omit for Wye connected meter.
Total Frequency	12	224	33	0.1 Hz	

7 Cybersecurity Requirements

7.1 Definitions

Solely for purposes of this Cybersecurity Requirements section, the following terms shall have the following meanings:

Confidential Data or **Confidential Information**. Information or data that, if disclosed to, or used by an unauthorized person, could provide an opportunity to gain an unwarranted economic advantage over others, or would have a significant adverse impact on the company's business, legal, financial or competitive position, or on its shareholders or employees. This includes all information acquired or generated by SCE that is protected by privacy laws, confidentiality COT Requirements, and legal privileges, including trade secrets.

Critical Energy Infrastructure Information or **"CEII".** Specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that: (1) relates details about the production, generation, transmission, or distribution of energy; (2) could be useful to a person planning an attack on critical infrastructure; (3) is exempt from mandatory disclosure under the Freedom of Information Act, and (4) gives strategic information beyond the location of the critical infrastructure.

Cyber Incident. (1) Any unauthorized access to, use of, or other breach in the security of IC's computing systems that (a) contain Edison Data, or any other accidental or unauthorized access to, interception of, acquisition, disclosure, use, modification, loss, damage, or destruction of Edison Data; or (b) causes any disruption to the business operations of SCE; or (2) if caused by the action or inaction of IC, any unauthorized access to, use of, or other breach in the security of Edison's Computing Systems, or any unauthorized access to, interception of, disclosure or acquisition of Edison Data caused by the action or inaction of IC or its affiliates.

Security Incident. Any unauthorized physical access to IC's facilities.

Edison's Computing Systems. SCE's and its affiliates' respective electronic computing and information systems, computers, servers, applications, files, electronic mail, electronic equipment, wireless devices, databases, data storage and other data resources, and SCE-sponsored connections to the internet communications network.

Edison Data. Any non-public information made available to IC by SCE whether or not designated by or on behalf of SCE as confidential information at the time it is provided or made available to IC, and all information IC derives from such information.

Edison Personal Information or **"EPI".** Any information in the possession or under the control of SCE or any of its affiliates, or that is furnished or made available by or on behalf of SCE to IC that identifies an individual, or that relates to, describes, or is capable of being associated with, an identifiable individual (whether a current or former SCE employee, customer, or otherwise), including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, government issued identification number, medical information, insurance information, education, employment information, financial identifiers or information, online account identifiers and password and/or security question together with the answer, or information regarding the individual's electric energy usage or electric service, including, without limitation, service account number, electricity demand, monthly billed revenue, credit history, rate schedule(s), meter data, or number or type of meters at a premise. EPI includes "personal information" as defined in The California Consumer Privacy Act, California Civil Code Section 1798.100 – 1798.199 and any regulations promulgated thereunder.

Industry Best Practices. Those practices, methods, and standards ("controls") which are expected from a skilled and experienced contractor with respect to the cybersecurity and privacy of data, systems, and other similar assets and which are implemented in a prudent and effective manner. These controls include, at a minimum, those consistent with leading technology and cybersecurity industry standards and frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST Privacy Framework, NIST 800 series, and the International Organization for Standardization (ISO) 27000 series.

IC's Computing Systems. Information systems and networks owned, operated, or leased by IC.

Technology Services. Telemetry or other data provided by IC.

7.2 Requirements Compliance

IC will implement reasonable administrative, technical, and physical safeguards, including any specific safeguards specified herein and from time to time by SCE, to protect the safety, security and integrity of the IC's and SCE's systems from unauthorized access, destruction, use, modification, or disclosure. IC will comply with the Cyber and Data Protection Requirements of this Section 7 and shall immediately notify SCE via email to Cybersecurity@sce.com if IC knows or reasonably believes that it is not in compliance with any of the Cyber and Data Protection Requirements.

7.3 Incident Disclosure

IC shall report to SCE any reasonably suspected or confirmed Cyber Incident or Security Incident as soon as reasonably practicable but in no event more than one (1) Business Day after IC becomes aware of the event. Such notification will be done via email to the Cybersecurity@sce.com and shall include the nature of the event, date and time of the event, suspected amount and type of information exposed (if applicable) and steps being taken to investigate the circumstances of the exposure. IC shall cooperate and assist SCE in the investigation, analysis and resolution of Cyber Incidents and Security Incidents. IC shall provide SCE with details of the investigation and final disposition of the Cyber Incident or Security Incident relevant to the services provided to SCE or which may impact the confidentiality, integrity or availability of those services or of Edison's Computing Systems or Edison Data.

7.4 Vulnerability Disclosure

In addition to the above, IC will use commercially reasonable efforts to: (x) regularly scan systems for vulnerabilities, (y) rank all vulnerabilities and promptly remediate detected vulnerabilities ranked as critical, high or moderate, and (z) use commercially reasonable efforts to identify any critical, high or moderate vulnerabilities, risks or threats that could potentially impact Edinson's Computing Systems or Edison Data, and shall notify SCE in writing within one (1) Business Day after such identification. If IC determines that it cannot remediate any such potential or detected vulnerabilities, risks or threats that could potentially impact Edison's Computing Systems or Edison Data within thirty (30) days after identifying any such potential or detected vulnerabilities, risks, or threats, it shall promptly notify SCE in writing. IC's notification shall provide detailed information describing the controls used to mitigate these such vulnerabilities, risks or threats.

7.5 Subcontractors

All IC requirements in the Cyber and Data Protection Requirements are also requirements for IC's subcontractors of any tier. IC is responsible for ensuring that, within six (6) months of the Amendment No. 2 Effective Date, its Subcontractors use commercially reasonable efforts to comply with the Cyber and Data Protection Terms and will be responsible for any Subcontractor breach of the Cyber and Data Protection Terms as though the breach was due to the acts or omissions of IC. IC shall ensure that (i) each Subcontractor provides timely notification and remediation of any Cyber Incident that involves such Subcontractor and (ii) such Subcontractor fully cooperates in any SCE investigation of a Cyber Incident involving the Subcontractor including audits as described in Section 11 ("Additional Audit Rights") below. IC shall immediately notify SCE if it knows or reasonably believes that any of its Subcontractors are not in compliance with the Cyber and Data Protection Terms.

7.6 Warranties and Representations

In addition to any other representations and warranties contained in the COT Requirements, and notwithstanding any statement in the COT Requirements limiting the applicable warranties, IC hereby represents and warrants that it has read and understood the Cyber and Data Protection Terms and that IC will be fully compliant with them prior to a connection with SCE.

7.7 Indemnification Obligations

IC shall indemnify, defend and hold harmless SCE and its affiliates, and SCE's and its affiliates' officers, directors, employees, agents, representatives, successors, and assigns from and against any and all losses, liabilities, damages and claims, and all related costs and expenses (including, but not limited to, any costs or expenses related to increased regulatory or administrative oversight), fines, penalties, or interest, including reasonable legal fees and costs, arising out of, in connection with, resulting from or relating to any claim relating to a breach of any of IC's obligations under the Cyber and Data Protection Terms.

7.8 Enforcement Expenses

IC shall pay, upon demand by SCE, all expenses, charges, costs and fees (including, without limitation, reasonable legal fees and costs) paid or incurred by or on behalf of SCE in connection with the enforcement of any of the rights of SCE or the obligations of IC or its Subcontractors resulting from or relating to any breach or reasonably suspected breach of the Cyber and Data Protection Terms.

7.9 LIMITATION OF LIABILITY FOR CYBER DAMAGES

ANY LIMITATIONS OF LIABILITY SET FORTH IN THE COT REQUIRMENTS, INCLUDING, BUT NOT LIMITED TO, LIMITATIONS OF LIABILITY WITH RESPECT TO CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY OR INDIRECT DAMAGES, LOST PROFITS OR OTHER BUSINESS INTERRUPTION DAMAGES OR TOTAL AGGREGATE DAMAGES, SHALL NOT APPLY TO DAMAGES ARISING OUT OF, IN CONNECTION WITH, RESULTING FROM OR RELATING TO IC OR ITS SUBCONTRACTOR'S BREACH OF ANY OF IC'S OBLIGATIONS UNDER THE CYBER AND DATA PROTECTION TERMS. SUCH DAMAGES SHALL HAVE NO LIMITATIONS OF LIABILITY.

7.10 Continuing Confidentiality and Non-Disclosure Obligations

To the extent IC possesses any Edison Data, IC shall treat such Edison Data in strict confidence, and IC may distribute or disclose such information only as specifically authorized in writing by SCE. IC's obligations shall apply regardless of whether such information falls within the definition of "Confidential Information" under the COT Requirements and shall continue until such time as SCE provides notice that such information may be distributed or disclosed without restriction. This shall survive the termination or expiration of and COT connection.

7.11 Additional Insurance

IC shall have insurance covering (a) liability arising from theft, dissemination and/or use of Confidential Information stored or transmitted in electronic form and (b) liability arising from a Cyber Incident. Such insurance will be maintained with limits of no less than $2,000,000 per claim and in the annual aggregate, and may be maintained on a stand-alone basis, or as part of any errors and omissions coverage required in the COT Requirements. This insurance shall have a retroactive date that equals or precedes the effective date of the applicable COT connection. IC shall maintain such coverage until the later of: (1) a minimum period of three years following termination or completion of the COT connection, or (2) until IC has returned or destroyed all Edison Data in its possession, custody or control, including any copies maintained for archival or record-keeping processes.

7.12 Physical and Environmental Security

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

7.13 Additional Audit Rights

SCE retains the right to audit IC and its subcontractors of any tier for adherence to the requirements of the Cyber and Data Protection Terms not more than once per year, or more often upon notification or reasonable belief by SCE of the occurrence of a Cyber Incident, or as required to comply with regulatory requirements. IC will cooperate with any such audit at IC's sole expense, other than the fees of any third-party auditor retained by SCE to conduct the audit.

Upon request, IC shall share the results of industry standard third-party audit reports (e.g., SOC 2 Type II audit, ISO 27001, or SSAE 16 audit) where available and in a timely manner.

7.14 Termination for Breach

If IC breaches, or through the act or omission of a subcontractor breaches, any of the Cyber and Data Protection Requirements, then SCE may in its discretion immediately terminate all connections and access provided to IC under the COT Requirements. IC will have a thirty [30] day opportunity to cure following IC's receipt of notice from SCE of such a breach or IC's notice to SCE of such a breach, whichever comes first. In such case that the breach is not cured within such thirty [30]-day period, the breach shall constitute a final termination of IC's agreements with SCE as an Event of Default and SCE shall not be responsible for any termination liability.

7.15 Rights in the Event of Breach

SCE shall have the right to bring suit in a court of competent jurisdiction against IC for a breach of the Cyber and Data Protection Requirements by IC (either directly or through the act or omission of a Subcontractor, its employees, agents or representatives) that compromises directly or indirectly SCE's cyber security.

7.16 Changes in Law

If, after the date hereof, either IC or SCE becomes aware of any changes in law related to the subject matter of the Cyber and Data Protection Requirements, upon notification by either Party to the other Party of such change, the Parties shall meet in good faith as soon as practicable to discuss achieving compliance with the changed legal requirements.

8 Cybersecurity And Data Protection Requirements

IC will use commercially reasonable efforts to: (i) implement and maintain appropriate measures, no less rigorous than privacy and cybersecurity Industry Best Practices, 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 SCE in its efforts to minimize risks to Edison’s Computing Systems and Edison Data and prevent unauthorized access to Edison’s Computing Systems and Edison Data, or unauthorized disclosure of Edison Data.

IC’s security and privacy practices and procedures must comply with the requirements:

(1) IC’s connection to SCE shall originate from a source based within the physical boundaries of the United States of America.

(2) IC personnel shall be physically located within the boundaries of the United States of America while supporting any systems that provide Technology Services to SCE.

(3) IC’s systems unrelated to providing Technology Services to SCE shall be logically isolated from the environment connecting to SCE.

(4) IC shall:

(a) Configure environment to use the most restrictive security settings available that do not directly interfere with IC’s ability to provide telemetry under these COT Requirements.

(b) Agree to and meet the requirements of the SCE Policy on Information Security, Cybersecurity, and Privacy for Suppliers:

- https://www.SCE.com/sites/default/files/inline-files/PolicyonInfoSecurityCybersecurityPrivacy.pdf

(c) Be onboarded with a review by SCE Cybersecurity that will include:

(i) Successfully completing a risk review performed by SCE Cybersecurity;

(ii) Meeting and maintaining the required Security Risk Score throughout the term of this COT Requirements; and

(iii) Providing details necessary to issue certificates from a Public Key Infrastructure (“PKI”) provider of SCE’s choosing for authenticating 2030.5 connections via Transport Layer Security (“TLS”) 1.2 or higher. This certificate must be used for connections to SCE from the IC.

(d) Use TLS 1.2 or higher with SCE issued certificate for all connections to SCE, including the following:

(i) Using SCE’s approved PKI certificate for Network authentication and communications encryption;

(ii) Supporting the ability to integrate with SCE’s approved PKI to rotate keys and certificates used in communication with SCE (via Enrollment over Secure Transport (“EST”) or Simple Certificate Enrollment Protocol (“SCEP”));

(iii) Supporting the ability to integrate with SCE’s approved PKI to check validity of Certificates (via Online Certificate Status Protocol (“OCSP”)); and

(iv) Supporting an ECC encryption specified by SCE during onboarding.

(e) Provide to SCE audit events, system events, and other events of interest logs. Logs can be delivered to SCE in a mutually agreed to automated way. If automation cannot be agreed to logs shall be retained for a minimum of three (3) years and delivered to SCE upon request.

(f) Provide firewall and network monitoring device logs used in the scope of service. Logs can be delivered to SCE in a mutually agreed to automated way. If automation cannot be agreed to logs shall be retained for a minimum of three (3) years and delivered to SCE upon request.

(g) Not access, host, manage, process, store, or use connections to SCE Computing Systems or SCE Information outside of the United States (such as, Onshore based data centers only).

(h) Provide a range of static network IP addresses for whitelisting:

(i) Unauthorized IP addresses will not allow SCE’s network connections;

(ii) IP addresses must be based in the United States of America; and

(iii) Any change to static IP addresses will require a 30-day advance notice.

(i) Direct all communications via designated intermediate device.

(j) If requested, provide validation of the Authenticity of IC’s information system components, including, but not limited to: detailed Bill of Materials, production locations, Hardware, Software and development processes, shipping and handling procedures, Configuration Management processes and personnel and physical security processes in the supply chain.

(k) Maintain an Information Security Program and Information Security policies designed and implemented to ensure the availability, confidentiality, integrity and reliability of the Technology Services managed by IC. This must include at minimum:

(i) Access Control, Identification and Authentication,

(ii) Application Development,

(iii) Auditing and Logging,

(iv) Configuration Management,

(v) Disaster Recovery and Business Continuity,

(vi) Encryption,

(vii) Incident Response,

(viii) Information Protection,

(ix) Information Security policies,

(x) Maintenance,

(xi) Mobile Device Security,

(xii) Monitoring,

(xiii) Network Security,

(xiv) Personnel Security,

(xv) Physical and Environmental Security,

(xvi) Security Patching,

(xvii) Security Risk Management,

(xviii) Technology Asset Management, and

(xix) Vendor Management

(l) Maintain Access Control, Identification and Authentication Services capable of:

(i) Uniquely identifying and Authenticating all Applications, devices, users and Services accessing information and systems used in support of Technology Services provided by the IC; and

(ii) Restricting, enforcing and minimizing access to those information and systems.

(m) Not share SCE-issued accounts, Authentication information or other SCE-issued access.

(n) Notify SCE within 24 hours when access is no longer required.

(o) Remove or disable access to information and computing systems within 1 business day for terminated personnel or transferred personnel who no longer require access to systems used to provide Technology Services.

(p) Maintain an Incident Response plan and notify SCE within 1 business day of a suspected or confirmed Cybersecurity Incident which could impact SCE.

(q) Encrypt all information used in support of Technology Services provided by the IC during transmission and while in storage or not in use.

(r) Maintain a policy prohibiting information used in support of Technology Services provided by IC from leaving the IC's Data Center, and/or worksite through the use of:

(i) Portable or removable media;

(ii) Devices with photographic capabilities; or

(iii) Paper.

(s) Implement controls (e.g., Information Security policies, a Code of Conduct, or confidentiality Agreements) to ensure IC personnel are aware of IC's Information Security program and procedures.

(t) Obtain written acceptance from IC's personnel annually of the following:

(i) IC's Code of Conduct, ethics policy, or confidentiality Agreement;

(ii) IC's Information Security policies; and

(iii) The requirements contained herein, unless provision contained in existing policies are substantially similar to the requirements contained herein.

(u) Maintain a Security Monitoring program for all IC and third-party technology used to provide Technology Services.

(i) The Security Monitoring program must include:

1. Monthly Security Vulnerability testing;
2. Quarterly Penetration Testing;
3. Intrusion Detection and Prevention Systems to identify and prevent attacks; and

(ii) A Data Loss Prevention solution to monitor electronic information.

(iii) Security Vulnerabilities must be ranked as critical, high, moderate or low.

(iv) Security Vulnerabilities ranked as critical, high and moderate must be remediated within 30 days of discovery or as soon as patching is available as applicable.

(v) Security Vulnerabilities ranked as low must be endeavored to be remediated within 180 days or as soon as patching is available as applicable.

(v) Upon request, provide SCE with security vulnerability testing and penetration testing results and remediation reports.

(w) Maintain IC's Computing Systems used in connection with IC's performance of its obligations under these COT Requirements must be logically isolated from all other IC Systems through the use of devices or solutions to restrict and limit the use of Ports and Services to only those required for operation and denying all other traffic by default.

(x) Maintain logical separation and isolation between the IC's or Third-Party technology used in connection with IC's performance of its obligations under these COT Requirements or used to access SCE Computing Systems and any IC or Third-Party technology used to provide Services to any of the IC's other customers, contractors or vendors.

(y) Ensure that all network connectors between IC and SCE are encrypted and routed as described herein.

(z) Maintain a personnel background investigation and verification program for all personnel with access to information or Computing Systems used in connection with IC's performance of its obligations under these COT Requirements. The background verification must identify if an employee has been convicted of a felony, property crime or fraud in any state where the individual has resided or worked during the past seven years and check the United States' Specially Designated Nationals List and the Denied Persons List.

(aa) Provide role-based Cybersecurity Awareness Training annually to all personnel.

(bb) Provide an annual Service Organization Control (SOC) 2 report, or provide an annual SOC 3 certification, or maintain ISO 270001 certification throughout the life any COT Connection.

(cc) Maintain a documented security patching program, processes and procedures. The security patching program must:

(i) Perform monthly, at minimum, security patching for all security vulnerabilities;

(ii) Provide detailed information describing the controls used to mitigate all un-remediated vulnerabilities; and

(iii) Notify SCE within 1 business day of any critical, high, or moderate security vulnerabilities that may impact Technology Services and cannot be remediated within 30 days. IC must also provide SCE with detailed information describing alternative controls that will be used to mitigate the un-remediated security vulnerabilities.

(dd) Assess, monitor and remediate all security risks associated with providing SCE with Technology Services.

(ee) Assess, monitor and remediate all security risks, including those associated with the IC's contractors, service providers and suppliers with access to Computing Systems used to provide SCE with Technology Services.

(ff) Meet or exceed supply chain risk and security standards and relevant executive orders such as, NIST SP 800-161, ISO 9001, E.O. 13873, and others as applicable to IC's provision of Technology Services.

(5) SCE may perform an audit of IC's adherence to the Policy on Information Security, Cybersecurity, and Privacy for Suppliers and the requirements contained herein as follows:

(a) SCE or its designee will perform the security audit.

(b) The audit will be performed on-site at IC's location.

(c) IC will provide access necessary to complete the audit to SCE or its designee.

9 Internet Requirements

IC Internet connection may be supplied by any service provider or medium that meets the following communications requirements:

a) IC Internet connection does not need to be a separate dedicated service for this solution and may be combined with an existing Internet service the customer already has available.

b) COT shall have a public static IPv4 address for SCE's use of AllowLists and BlockLists.

c) IC Internet connection shall not exceed 200 milliseconds (ms) latency (delay) for the one-way transmission of data between the COT GW and SCE's headend 2030.5 servers.

d) IC Internet connection requires a minimum of 2 Megabits per second (Mbps) bandwidth reserved for telemetry functions.

e) IC Internet connection shall not exceed 1% packet loss to ensure acceptable communications performance.

f) If IC selects an Internet service provider using a metered service, the IC is responsible for any overage costs.

g) IC Internet router shall be patched regularly with patches and software upgrades used only from the authorized vendor repositories.

h) The IC is RESPONSIBLE for safeguarding their internal networks (logically and physically) to protect the equipment and systems from unauthorized access and manipulation.

10 Cellular Strength

IF the IC solution will be using a cellular connection to the internet, then:

a) SCE REQUIRES that Reference Signal Received Quality (RSRQ) values be greater than -14 dB with corresponding Reference Signal Received Power (RSRP) values, as listed in Figure 3 below. (SCE USES the Berkeley Varitronics Systems[6] – Octopus Cellular Signal Meter Pro Kit to measure cellular signal strength.)

b) DO NOT INSTALL anything less than RSRQ values of -14 dB.

   a. NOTE the negative signs and that greater than in relative terms means a smaller number

Table 2- Cellular Signal Strength Requirements
Using Berkeley Varitronics Systems - Octopus Cellular Signal Meter Pro Kit

If RSRQ (dB) is=	Then RSRP (dBm) must be:
≥ -9	≥ -105
-10	≥ -104
-11	≥ -103
-12	≥ -102
-13	≥ -91
-14	≥ -87
-15	NA - Do Not Install
-16	NA - Do Not Install
-17	NA - Do Not Install
-18	NA - Do Not Install
-19	NA - Do Not Install

11 Approved COT GWs and Aggregators

SCE's approved COT GWs and aggregators that have been tested for interoperability with SCE's IEEE 2030.5 CSIP certified DERMS GW can be found at: https://www.sce.com/business/smart-energy-solar/solar-for-business/grid-interconnections/interconnecting-generation-under-rule-21.

Interconnection customers are allowed to propose using other gateways or aggregator vendors. Gateways and aggregator vendors that have not yet been approved by SCE are subject to interoperability testing and approval with SCE's IEEE CSIP certified DERMS GW. This would result in additional time and cost for the IC.

In cases where a vendor is seeking GW or aggregator interoperability approval, or if an IC wishes to use a GW or aggregator not yet approved for interoperability by SCE, SCE will provide a cost estimate and timeline to complete testing and evaluation of the requested device. For more information, contact: Rule21@sce.com.

- End of COT Procedures -

[6] https://www.bvsystems.com/

Annex 1 – Approved COT GWs and Aggregators

SCE has tested and certified the customer-owned telemetry (COT) vendors shown below for interoperability with SCE's Common Smart Inverter Profile (CSIP) certified IEEE 2030.5 solution and DERMS. The list of certified-interoperable vendors is expected to expand as SCE continues to work with vendors to provide COT solutions.

Interconnection customers (ICs) are free to propose other vendors with CSIP-certified gateways or other aggregators; however, any newly proposed GW or aggregator would be required to be tested and configured for interoperability with SCE's DERMS, which may require additional time and, in some cases, could delay the ICs expected online date of their generating facilities. SCE highly recommends that ICs proposing new gateways proactively reach out to SCE to initiate the testing and configuration required to approve their proposed gateway. In their proposal, the IC should provide relevant documentation regarding the new gateway, configuration, or use case to inform SCE'S review and testing determinations. Such documentation must include technical specifications, descriptions of the proposed gateway, configuration options, and relevant functionality that SCE might wish to test, as well as confirmation whether the gateway is commercially available.

Entities that want to become aggregators, or vendors wishing to certify interoperability of their GWs with SCE's DERMS, should contact SCE at Rule21@sce.com to initiate the testing and approval process.

The following are certified-interoperable COT vendors:

Approved COT GWs and Aggregators

Remote Site Gateway Device	Aggregator
Applied Systems Engineering Inc. (ASE a Kalkitech Company) Quotes / Ordering Email: sales@ase-systems.com Support: support@ase-systems.com Engineering / SCADA Testing: DER-Support@ase-systems.com Phone: 408-364-0500 Website: https://www.ase-systems.com/utility-interconnection-gateway/	**Kitu Systems, Inc.** Email: sales@kitu.io Phone: 619-569-2208 x2 Website: www.kitu.io

DISCLAIMER: SCE does not endorse any vendor, product, or service but certifies the interoperability of their devices or services with SCE's IEEE 2030.5 headend server. SCE does not attest to the cybersecurity and cyber hygiene of, or recommend, any certified interoperable vendor. The material and information presented herein is not exhaustive, and readers should not rely upon the material or information as a basis for making any business, legal, or any other decision.

Please note that this document provides links to other websites that may have different terms of use and privacy policies. Please refer to those websites and mobile applications for the appropriate information; SCE has no control over the content of these third-party websites and mobile applications. In addition, a hyperlink to a non-SCE website or link to access a third-party mobile application does not mean that SCE endorses or accepts any responsibility for the content, or the use, of the website or mobile application. If you decide to access any of the third-party websites or mobile applications linked to this website, you do so entirely at your own risk.

SCE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESSOR IMPLIED, WITH REGARD TO THIS DOCUMENT OR INFORMATION HEREIN, THIRD-PARTY PRODUCTS, THIRD-PARTY CONTENT OR ANY SOFTWARE, EQUIPMENT, OR HARDWARE FROM THIRD-PARTIES.

REVISION NOTES

Date	Notes / Revisions
August 11, 2025	New Annex 1 to SCE’s Customer-Owned Telemetry Procedures