

Customer-Owned Telemetry (COT) Procedure

SUMMARY

As required by California Public Utilities Commission (CPUC) [Resolution E-5038, "Approval, with Modifications, of Rule 21 Telemetry Requirements Proposed in Compliance with Decision 19-03-013."](#) Ordering Paragraph 2, PG&E approves the use of customer-owned telemetry (COT) to support distribution-connected generating facilities' telemetry requirements, effective October 4, 2021.

Generating facilities can purchase COT from certified-interoperable vendors. These vendors are compliant with the Institute of Electrical and Electronics Engineers (IEEE) 2030.5, "Standard for Smart Energy Profile Application Protocol," and [Common Smart Inverter Profile \(CSIP\)](#) implementation, as specified in [Electric Rule 21, "Generating Facility Interconnections."](#)

Certified-interoperable vendors' COT devices or aggregator connections have also been tested to be compatible within PG&E's IEEE 2030.5 infrastructure and to meet PG&E equipment requirements. See [Attachment 1, "Certified-Interoperable Customer-Owned Telemetry Vendors."](#) for the list of certified-interoperable vendors.

Level of Use: Information Use

TARGET AUDIENCE

The target audience is PG&E electric grid interconnection (EGI) interconnection customers (ICs) who use COT that communicates using IEEE 2030.5 protocol to PG&E to fulfill their telemetry requirements. The telemetry requirement is typically for ICs with generation or storage devices with a total aggregate generation of 1 Megawatt (MW) or larger. COT is approved only for distribution-connected ICs with a telemetry requirement and no other protection requirements.

SAFETY

This utility procedure describes administrative tasks that do not expose personnel to any significant hazards.

BEFORE YOU START

NA

Customer-Owned Telemetry (COT) Procedure

TABLE OF CONTENTS

SECTION	TITLE	PAGE
1	IC Application to Interconnect – YourProjects Application	2
2	Metering Configuration	3
3	Required Data Points	4
4	COT Specifications	6
5	Cybersecurity Requirements	9
6	COT Maintenance Specifications	11
7	Cellular Signal Strength.....	12
8	Frequently Asked Questions	12

PROCEDURE STEPS

1 IC Application to Interconnect – YourProjects Application

- 1.1 The IC APPLIES to interconnect their proposed generation through YourProjects application portal.
- 1.2 IF the IC has a project interconnecting onto the distribution grid that is 1 megawatt (MW) or greater (according to the system nameplate),

THEN the customer SELECTS one of the following three options:

- Customer-owned telemetry – remote site gateway
- Customer-owned telemetry – aggregator
- PG&E MiniRTU

- 1.3 PG&E personnel STUDY proposed generation AND PROVIDE a study report to the IC.
- 1.4 The IC REVIEWS the study report AND REQUESTS an interconnection agreement (IA) from PG&E.
- 1.5 The EGI contact PERFORMS the following tasks:
 1. TENDER IA to the IC.
 2. REQUEST a choice in vendor (SEE [Attachment 1, “Certified-Interoperable Customer-Owned Telemetry Vendors”](#)).
 3. TENDER Work Requested by Others (WRO) agreement, based on a \$4,000 flat cost for configuring the COT solution.

Customer-Owned Telemetry (COT) Procedure

- 1.6 The IC PROCEEDS as follows:
1. CHOOSE a vendor.
 2. SIGN the IA.
 3. RETURN the IA AND REPLY with their vendor choice to the EGI contact.
 4. SIGN AND RETURN the WRO agreement.
- 1.7 Once the WRO agreement is signed AND payment is received, the EGI contact ASSIGNS an IT project manager for the proposed generation site.
1. The IT project manager ASSISTS with coordinating the configuration of the COT to PG&E's system.
- 1.8 The IC WORKS with the vendor to install the COT at their site, in accordance with required metering points set in [Section 3, "Required Data Points,"](#) on Page 4.
- 1.9 The IT project manager COORDINATES the configuration of the COT onto PG&E's system.
- 1.10 When all systems are working correctly and other required site work and testing are successfully completed, the EGI contact PROVIDES the Permission to Operate (PTO) to the IC.

2 Metering Configuration

- 2.1 To uncover masked load and support PG&E distribution control center (DCC) switching operations, sites requiring telemetry (typically 1 MW or larger) must PROVIDE aggregate metering of each distributed energy resource (DER) type (e.g., the sum of all individual solar onsite).
- 2.2 The following data points are required at each point shown in [Figure 1, "Required Site Metering Examples,"](#) on Page 4 for the COT solution, depending on installed generation resources:
- **M1:** Site (Point of common coupling measurements).

NOTE

M1 is optional, to provide PG&E additional information OR as monitoring point if there is only one generator fuel type AND no other load onsite.

- **M2:** Photo-voltaic (PV) Solar (aggregate of all PV on site)
- **M3:** Battery Energy Storage System (BESS) (aggregate of all storage onsite)
- **M4:** Fuel Cell (aggregate of all fuel cell generation on site)

Customer-Owned Telemetry (COT) Procedure

- **M(n):** Any other Generation Type (aggregate of any other generation type not listed above)

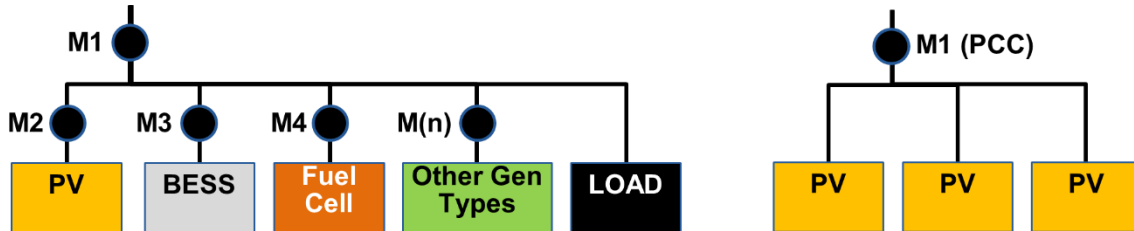


Figure 1 Required Site Metering Examples

3 Required Data Points

3.1 Program Description

1. As a condition to PG&E issuing the final PTO for generator interconnection projects requiring telemetry (typically 1 MW or larger), the IC SUPPORTS PG&E's implementation of COT to provide the following real-time data from the generating facility to PG&E to satisfy Producer's Rule 21 DER telemetry requirements:
 - 3-phase and total watts (W)
 - 3-phase and total volt-amperes-reactive (VAR)
 - 3-phase voltage (V)
 - 3-phase amperes (Amps)
2. TEST monitoring functionality at the generating facility.
 - a. COORDINATE the day and time for functionality testing with the IC, to ensure minimal to no impact on existing operations.
3. During the Operational Period, the IC must MAINTAIN the following items:
 - a. The connection between the COT and its equipment.
 - b. The accurate scaling of watts, VARs, volts, and amps values.
 - (1) IF the IC CHANGES Item a or Item b above, and such change results in values that do not accurately reflect local conditions,

THEN the IC must RESOLVE the issue within 2 weeks of notice or discovery of the issue. Parties AGREE that the IC remains solely responsible for its obligations under these requirements and the Generating Facility Interconnection Agreement (GFIA).

Customer-Owned Telemetry (COT) Procedure

4. During the Operational Period, the IC must NOTIFY PG&E 10 days in advance of making any changes to the telemetering devices connected to the COT.
 - a. EMAIL DERComms@pge.com AND DESCRIBE the proposed change.
5. During the Operational Period, the IC is RESPONSIBLE for connections with the COT equipment.
6. [Table 1](#) below describes the required data points for locations M1, M2, M3, M4, ..., M(n), as applicable.
 - M1 is optional, to provide PG&E additional information OR as monitoring point if there is only one generator fuel type AND no other load onsite.

Table 1 Directly Monitored Telemetry Points by Generation Type from the DER Site

Telemetry	Accumulation Behavior Type	Commodity Type	Data Qualifier Type	Flow Direction Type	Kind Type	Phase Code	Uom Type	Unit and Precision	Notes
Current A	12	0	0	0	0	128	5	1 A	Always Positive
Current B	12	0	0	0	0	64	5	1 A	Always Positive
Current C	12	0	0	0	0	32	5	1 A	Always Positive
Voltage AN	12	0	0	0	0	129	29	0.1 V	Use for Wye connected meter. Omit for Delta connected meter.
Voltage BN	12	0	0	0	0	65	29	0.1 V	Use for Wye connected meter. Omit for Delta connected meter.
Voltage CN	12	0	0	0	0	33	29	0.1 V	Use for Wye connected meter. Omit for Delta connected meter.
Voltage AB	12	0	0	0	0	132	29	0.1 V	Use for Delta connected meter. Omit for Wye connected meter.
Voltage BC	12	0	0	0	0	66	29	0.1 V	Use for Delta connected meter. Omit for Wye connected meter.
Voltage CA	12	0	0	0	0	40	29	0.1 V	Use for Delta connected meter. Omit for Wye connected meter.
Active Power Total	12	0	0	0	0	224	38	1 W	Negative = Export to Grid
Active Power A	12	0	0	0	0	128	38	1 W	Negative = Export to Grid
Active Power B	12	0	0	0	0	64	38	1 W	Negative = Export to Grid
Active Power C	12	0	0	0	0	32	38	1 W	Negative = Export to Grid
Reactive Power Total	12	0	0	0	0	224	63	1 VAR	Negative = Capacitive Load
Reactive Power A	12	0	0	0	0	128	63	1 VAR	Negative = Capacitive Load
Reactive Power B	12	0	0	0	0	64	63	1 VAR	Negative = Capacitive Load
Reactive Power C	12	0	0	0	0	32	63	1 VAR	Negative = Capacitive Load

Customer-Owned Telemetry (COT) Procedure

4 COT Specifications

4.1 The following are the **functional** specifications for the COT equipment:

1. COT must be CSIP-certified for IEEE 2030.5.
2. COT must run the latest version of CSIP implementation of 2030.5 (Currently, CSIP 2.1 – March 2018).
3. COT must be able to update the CSIP 2030.5 version, and the version should be verifiable.
4. COT must have proven interoperability with the PG&E CSIP-certified IEEE 2030.5 Head-end system.
5. COT must be able to translate between the CSIP implementation of IEEE 2030.5 and the local device protocol for providing telemetry information.
6. COT must be able to provide metering point values (e.g., W per phase and total, VAR per phase and total, voltage per phase, Amps per phase) at any uniquely identified input with the appropriate CSIP characteristics (RoleFlags, ServiceCategoryKind, AccumulationBehaviour, Commodity, DataQualifier, FlowDirection, PowerOfTenMultiplier, Qualityflags, etc.).
7. COT must monitor status values (e.g., alarm or status points) at any uniquely identified input.
8. COT must post data at a minimum of every 30 seconds, as defined by the posting rate given by the PG&E 2030.5 Headend server.
9. Data must be scaled appropriately based on units of measure (kW, MW, etc.).
10. COT must be able to receive input signals from one or more serial and Internet Protocol (IP) connections.
11. COT must have methods to configure the site and site DER/load identification information.
12. COT must have methods to configure data values as required for each measurement location within a site.
13. COT must have methods to configure protocol parameters, as required.
14. COT must have methods to configure security parameters, as required, including user access management.
15. COT must have methods to configure communication and network parameters, as required.

Customer-Owned Telemetry (COT) Procedure

16. COT must have methods to configure alarm parameters, as required.
17. COT must provide continuous monitoring of connections to local DER or metering interfaces.
18. The device must automatically restart to full functionality after power is restored following the complete loss of power to the COT equipment.

4.2 The following are the **non-functional** specifications for the COT equipment:

1. Gateway should be an operating system (OS)-embedded type of device. Currently, PG&E does not accept Windows 10 Enterprise operating system for a Gateway. The vendor must indicate what security certification, such as ISO/IEC 15408 Common Criteria (CC) and Evaluation Assurance Level (EAL), the OS has achieved from an external-auditing organization.
2. Minimum operating temperature range: -20° C to +70° C.
 - a. Preferred operating temperature range: -40° C to + 85° C.
3. Gateway is capable of being installed inside an outdoor cabinet.
4. COT must meet all IEEE 2030.5 mandatory requirements described in the standard and must follow the IEEE 2030.5 Implementation Guide for the Common Smart Inverter Profile (CSIP 2.1), acting as a DER Client or Aggregator when communicating with the PG&E DER Headend server using CSIP IEEE 2030.5.
5. COT must initiate all communications with the PG&E DER Headend Server according to polling and posting intervals provided by the server, to ensure the Gateway has up-to-date settings and PG&E understands the operational state of the Gateway.
6. The default posting rate must be every 30 seconds and must be configurable.
7. Transport Layer Security (TLS) must be used for all Hypertext Transfer Protocol Secure (HTTPS) transactions, and the Gateway must support a cipher suite that is compliant with TLS 1.2 or above.
 - a. The Gateway provider and PG&E's head-end service provider must mutually AGREE on the specific cipher suite.
8. A valid certificate must be used in IEEE 2030.5 TLS transactions. The COT must have a "SunSpec PKI" issued device certificate and store key files using secure methods.
9. COT must perform mutual authentication (Two-Way Authentication) during the TLS handshake by exchanging and authenticating with the DER Headend Server's certificate. The DER Headend server hashes the COT certificate and validates it with the pre-registered SFDI/LFDI of the COT.

Customer-Owned Telemetry (COT) Procedure

10. COT must provide a stable communication path via public internet to communicate with PG&E DER Headend Servers.
11. COT must support access control functions, including Gateway applications checking the Personal Identification Number (PIN) code from the registration message.
12. COT must support the following methods to get the PG&E IEEE 2030.5 DER Headend Server's "DeviceCapability" resource:
 - a. Out-of-Band Discovery: Gateway can be provisioned with all the DER Headend information by an out-of-band method.
 - b. Unicast-DNS and DNS-SD: Gateway is provisioned with the Domain Name System (DNS) name of the PG&E Headend server. The Gateway must perform name resolution using DNS and using DNS based Service Discovery (DNS-SD) to get the PG&E DER Headend Server IP address and port, scheme (HTTPS), and the path to the "DeviceCapability" resource.
13. Once the COT gets its EndDevice instance, it finds its group assignments by following the "FunctionSetAssignmentListLink." The COT periodically polls these resources at a rate specified by the DERProgramList:pollRate setting.
14. COT must support operating with no Function Set Assignment for telemetry-only installations.
15. The PG&E DER Headend server uses the "Time" function set (IEEE 2030.5) to distribute the current time to the Gateway. The Gateway must update the local time of the device to this time.
16. Communication performance requirements for the interfaces to the DER Headend Server are listed below. These requirements do not constrain or define the performance of various communication systems.
 - a. Availability of Communication: Must be active and responsive whenever the end device is operating and in a continuous operating region or mandatory operating region.
 - b. Reporting Telemetry Data: Post data every 30 seconds. This is based on the default posting interval from the PG&E DER Headend Server.
 - c. Reporting Status Information: <=10 seconds. This is based on the maximum amount of time to report status information after receiving status information from an end device.
 - d. Reporting Alarm: <=10 seconds. This is based on the maximum amount of time to report alarms after detecting and/or receiving alarms from an end device.

Customer-Owned Telemetry (COT) Procedure

17. COT must have sufficient public documentation regarding the following:

- a. System Installation Guide
- b. System Administrator Guide
- c. User (Operator) Guide
- d. Functional Specifications and Related Technical Specifications
- e. System Configuration Hardening Guide

5 Cybersecurity Requirements

5.1 PG&E PROVIDES network access to ICs to supply power and related telemetry data originating from an IC's DER system.

1. Access is governed by the security requirements defined in this procedure.
2. IF the IC violates any terms of this agreement, as described in [Subsection 5.2](#) below, THEN PG&E may REVOKE access.

5.2 Any IC connecting to PG&E networks must COMPLY with the security requirements described in this procedure to ensure the confidentiality, integrity, and availability of PG&E networks, systems, and data.

1. General Information

- a. Certified-interoperable gateway vendors must be ABLE to communicate with PG&E's IEEE 2030.5 system using TLS 1.2 or above.
 - (1) The Gateway vendor and PG&E's head-end service provider must mutually AGREE on the specific cipher suite.
- b. The IC connecting to PG&E networks and systems must FOLLOW security principles and guidance, based on the then-current National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) framework; currently, NIST 800 53 r4 OR similar security frameworks.

2. Identity and Access Management

- a. The IC must ENSURE that individuals operating the DER or accessing assets connected to the PG&E network are properly authenticated and have documented roles and responsibilities governing their level of access.
- b. All IC devices accessing the PG&E networks and systems must have valid credentials identifying the asset.

Customer-Owned Telemetry (COT) Procedure

- c. ENSURE that all assets and devices are physically protected to prevent unauthorized access and use.
- 3. Network and Asset Protection
 - a. The IC DER systems or Local Area Networks (LANs) connecting to the PG&E IEEE 2030.5 systems must have adequate technical controls (perimeter firewalls, anti-virus protection, etc.).
 - b. The IC must SAFEGUARD their internal networks (logically and physically) to protect the equipment and systems from unauthorized access and manipulation.
- 4. Cyber Event Detection
 - a. PG&E must EMPLOY tools and techniques to detect and remediate cyber risks.
 - (1) The IC AGREES that when a cyber event is detected, PG&E must PERFORM problem analysis including monitoring, scanning, and auditing of PG&E networks (and traffic to such PG&E networks).
 - (2) PG&E must COORDINATE such problem analysis with the IC in advance, initiating from PG&E sites or the IC site with the agreement of the IC.
 - (3) The IC is responsible for any tools and techniques to DETECT AND REMEDIATE cyber risks within their networks or connections AND PERFORMS their own analysis.
 - (4) The IC can REQUEST reporting or results of investigations or events.
 - b. The IC must PROVIDE, upon PG&E request, systems log and audit trails in support of PG&E cyber event detection and/or cyber event analysis or forensic analysis.
 - (1) PG&E can REQUEST additional data to support the analysis of IC infrastructure connections to PG&E networks to confirm that the connection is authorized, and that the IC has implemented cyber safeguards and best practices, including implementation of appropriate firewall, patch, and anti-virus measures.
 - (2) The IC may also REQUEST that PG&E provide systems logs and audit trails in support of PG&E cyber event detection and/or cyber event analysis or forensic analysis.
 - a. PG&E LIMITS the scope of their monitoring, scanning, and auditing activities to ensure compliance with these requirements AND COORDINATES with designated members of the IC information security staff in advance.

Customer-Owned Telemetry (COT) Procedure

- (1) The IC CONSENTS to such monitoring, scanning, and auditing.
- (2) PG&E KEEPS in strict confidence any proprietary or other information of the IC obtained through monitoring, scanning, and auditing.
- (3) PG&E DOES NOT DISCLOSE this information to third parties, AND USES it only for the purposes set forth in this [Section 5.2.4.c](#).

5. Cyber Event Response

- a. The IC must HAVE a documented and tested Cyber Incident Response Plan (IRP) or a documented process, so that in the event of a confirmed cyber event the IC can notify PG&E and provide information and the scope of exposure.
 - (1) PG&E must HAVE a similar plan AND/OR process to notify the IC and provide information on the scope of exposure, extent of conditions, etc.
- b. The IC is RESPONSIBLE for all network activities that originate from its facilities, systems, or networks that pass into PG&E networks.
 - (1) In case of a cyber event, PG&E may REQUEST additional logical or administrative controls be deployed as precautionary and risk mitigation measures.
- c. Upon completion of a cyber event investigation and indication of criminal activity, PG&E in conjunction with the IC, must PROVIDE evidence to the appropriate law enforcement or regulatory agencies.

6 COT Maintenance Specifications

6.1 The customer or their contracted vendor has the following responsibilities:

1. MAINTAIN customer-owned equipment in good working order.
2. MANAGE all firmware and security patching of customer-sited telemetry equipment.
3. REPAIR OR REPLACE malfunctioning equipment within 30 days. Security-related patching may be required in a shorter timeframe.

6.2 Gateway must have an encrypted interface for remote management to upgrade software/firmware, install security patches, and reboot device remotely.

Customer-Owned Telemetry (COT) Procedure

7 Cellular Signal Strength

7.1 To ensure PG&E is receiving quality data from the site, VERIFY the cellular signal strength is in the required range for the program.

7.2 IF the COT solution is using a cellular connection to the internet, THEN:

1. PG&E REQUIRES that Reference Signal Received Quality (RSRQ) values be greater than -14 dB with corresponding Reference Signal Received Power (RSRP) values, as listed in [Table 2](#) below. (PG&E USES a tool from [Berkeley Varitronics Systems](#) to measure cellular signal strength.)
2. DO NOT INSTALL anything less than RSRQ values of -14 dB.
 - a. NOTE the negative signs; “greater than” symbol in relative terms means a smaller number.

Table 2. Cellular Signal Strength Requirements *

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

8 Frequently Asked Questions

8.1 **Question:** What is the estimated cost of the new COT solution?

Answer: Costs for COT include the following:

- \$4,000 for configuring the customer-owned gateway to the PG&E server.
- Any costs that vendors charge for the procurement, installation, and support of the COT solution.

* Using Berkeley Varitronics Systems testing tool

Customer-Owned Telemetry (COT) Procedure

The goal of the system is to estimate utility-related costs for the new telemetry solution at less than \$20,000 for ICs, including PG&E and vendor-related costs. This does not include recurring third-party telecom costs.

8.2 **Question:** What is the best way to power the remote site gateway?

Answer: Power the COT from the utility side of any breaker or disconnect device and not from the DER side. This avoids requiring permission to operate for the DER before configuring and testing the COT with PG&E's network.

END of Instructions

DEFINITIONS

Aggregator: IEEE 2030.5 aggregator server that communicates telemetry data points from one or more customer interconnection sites to PG&E's IEEE 2030.5 server.

Distribution-connected: Connected to PG&E's distribution system, which is the portion of PG&E's power system that is at voltage less than 60 kilovolt (kV).

Point of Common Coupling (PCC): The transfer point for electricity between the electrical conductors of distribution provider and the electrical conductors of producer.

Remote Site Gateway (RSG): IEEE 2030.5 site gateway device that communicates telemetry data points to PG&E's IEEE 2030.5 server.

Utility-related costs: The Smart Inverter Working Group One Final Report defines utility-related costs as "charges for metering equipment (meters, circuit transformers [CT] and potential transformers [PT]), communications/telemetry equipment (Remote Terminal Unit [RTU] and a modem), and charges for labor, taxes, and maintenance."

IMPLEMENTATION RESPONSIBILITIES

Manager for Electric Grid Interconnection (EGI) retail is responsible for the front-end processes.

The Advanced Distribution Management System (ADMS) Business Support team is responsible for commissioning systems.

The Distributed Energy Resources Management Systems (DERMS) support group is responsible for overall system support, and for evaluating new COT that are not included in the certified-interoperable vendor list in [Attachment 1](#).

GOVERNING DOCUMENT

NA

Customer-Owned Telemetry (COT) Procedure

COMPLIANCE REQUIREMENT / REGULATORY COMMITMENT

Information and Records Management:

PG&E data, information, and records are company assets that must be traceable, verifiable, accurate, and complete and can be retrieved upon request. Functional areas are responsible for complying with the Information & Records Governance Policy, standards, and the Information and Records Retention Schedule. Refer to [GOV-7101S, "Enterprise Records and Information Management Standard,"](#) for further guidance or contact Information & Records Governance at Information&RecordsGovernance@pge.com.

REFERENCE DOCUMENTS

Developmental References:

NA

Supplemental References:

[Berkeley Varitronics Systems](#)

[California Public Utilities Commission \(CPUC\) Resolution E-5038, "Approval, with Modifications, of Rule 21 Telemetry Requirements Proposed in Compliance with Decision 19-03-013"](#)

[Common Smart Inverter Profile \(CSIP\) – IEEE 2030.5 Implementation Guide for Smart Inverters \(published by SunSpec Alliance\)](#)

[Electric Rule 21, "Generating Facility Interconnections"](#)

[YourProjects Application Portal](#)

APPENDICES

NA

ATTACHMENTS

[Attachment 1, "Certified-Interoperable Customer-Owned Telemetry Vendors"](#)

DOCUMENT REVISION

This procedure supersedes Utility Procedure TD-2306P-01, "Customer-Owned Telemetry (COT) Procedure," Rev. 0, dated 06/13/2022.

Customer-Owned Telemetry (COT) Procedure**DOCUMENT APPROVER**

Alex Collins, Manager, DERMS Execution and Operations

Rene Aguirre, Senior Manager, ADMS Business Support

Leesa Miner, Manager, Electric Grid Interconnection Retail

DOCUMENT OWNER

Alex Collins, Manager, DERMS Execution and Operation

Denise Zack, Business Process Analyst, Electric Grid Interconnection Tools and Operational Support

DOCUMENT CONTACT

Denise Zack, Business Process Analyst, Electric Grid Interconnection Tools and Operational Support

Rustom Dessai, Principal Grid Innovation Engineer, Clean Energy Technology Platforms

REVISION NOTES

Where?	What Changed?
Throughout	Spelled out acronyms and provided complete references; updated links. Changed “approved vendors” to “certified-interoperable vendors.”
Subsection 3.1	Removed old Table 2 (consolidated redundant tables for data points).
Section 4	Consolidated Sections 4 and 5 under one title – “Section 4. COT Specifications.” Subsection 4.1 provides functional specifications, Subsection 4.2 – non-functional.
Subsection 4.1	Removed old Item 6 that mentioned Attachment 2 (Gateway must be able to provide the LogEvents). Removed old Item 11 (COT must have the ability to determine the average, minimum, and maximum from a set of values).
Subsection 4.2	Updated Item 7 (changed protocol to TLS 1.2 and added requirement for Gateway vendor and PG&E head-end service provider to mutually agree on cipher suite.). Updated Item 10 (removed requirement for Static IPs). Updated Items 16.c and 16.d – changed timing to <= 10 seconds.
Step 5.2.1.a	Specified TLS version number of 1.2 or above; added requirement for Gateway vendor and PG&E head-end service provider to mutually agree on cipher suite.

Customer-Owned Telemetry (COT) Procedure

Where?	What Changed?
Subsection 7.2	Figure 3 became Table 2.
Definitions	Added "Aggregator."
Implementation Responsibilities	Removed an item related to SCADA supervisor. Changed responsibility for overall system support from EGI senior manager to DERMS support group. Added ADMS business support item for commissioning systems.
Compliance Requirement / Regulatory Commitment	Provided updated statement for Information and Records Management.
Reference Documents	Listed references mentioned within the procedure.
Attachments	Removed Attachment 2.
Document Approver, Document Owner, Document Contact	Updated names and titles.