CALIFORNIA INDEPENDENT SYSTEM OPERATOR

AND

PACIFIC GAS AND ELECTRIC COMPANY

COORDINATED FUNCTIONAL REGISTRATION AGREEMENT

COORDINATED FUNCTIONAL REGISTRATION AGREEMENT

This Coordinated Functional Registration Agreement ("Agreement") is entered into by and between the California Independent System Operator Corporation, a California non-profit public benefit corporation ("ISO") and Pacific Gas and Electric Company (the "Transmission Entity" or "TE"). In this Agreement, the ISO and TE are jointly referred to as the "Parties" and individually as a "Party."

RECITALS

WHEREAS, the Energy Policy Act of 2005 was signed into law in August 2005, which added a new Section 215 to the Federal Power Act giving the Federal Energy Regulatory Commission ("FERC") authority over developing and enforcing Reliability Standards for the Bulk Power System;

WHEREAS, in Docket RM06-16-000, 118 FERC ¶ 61,218 ("Order No. 693"), FERC approved various Reliability Standards applicable to users, owners and operators of the Bulk Power System developed by the North American Electric Reliability Corporation ("NERC"), the entity certified by FERC as the Electric Reliability Organization ("ERO"), and FERC has since then continued to approve additional and modified Reliability Standards;

WHEREAS, the NERC, through the Western Electricity Coordinating Council ("WECC") Delegation Agreement (filed with FERC in Docket No. RR07-7) has delegated authority to the WECC for the purposes of proposing Reliability Standards to the ERO and enforcing Reliability Standards within the WECC;

WHEREAS, the ISO is registered with the NERC as a Transmission Operator ("TOP") with respect to certain transmission facilities under its operational control in accordance with the NERC compliance registry process and is responsible for complying with certain Reliability Standards that are subject to enforcement by the Compliance Enforcement Authority designated by the NERC;

WHEREAS, the TE owns and maintains certain transmission facilities that are part of the Bulk Power System, is registered with the NERC as a TOP with respect to those facilities in accordance with the NERC compliance registry process, and is responsible for complying with certain Reliability Standards that are subject to enforcement by the Compliance Enforcement Authority designated by NERC; and

WHEREAS, the Parties intend by this Agreement to effectuate a Coordinated Functional Registration, as provided for in Rule 508 of the NERC Rules of Procedure, specifying their respective compliance responsibilities as TOPs for the transmission facilities covered by this Agreement.

AGREEMENT

NOW THEREFORE, in view of the recitals set forth above, which the Parties acknowledge and agree are accurate representations of the facts and are hereby incorporated by reference, the ISO and TE agree to the terms of this Agreement as set forth herein.

1. DEFINITIONS.

Unless otherwise defined herein, all capitalized terms shall have the meaning set forth in the FERC-approved NERC Glossary of Terms or the definitions appendix for the NERC Rules of Procedure.

"ISO Tariff" means the California Independent System Operator Corporation Operating Agreement and Tariff, dated March 31, 1997, as it may be modified from time to time.

"Confidential Information" means (i) all materials marked "Confidential," "Proprietary" or with words of similar import, and (ii) all observations of equipment (including computer screens) and oral disclosures related to either Party's systems, operations and activities that are indicated as such at the time of observation or disclosure, that are provided to either Party by the other Party in connection with performing the Parties' responsibilities as set forth in this Agreement. Confidential Information includes portions of documents, records and other material forms or representations that either Party may create, including but not limited to, handwritten notes or summaries that contain or are derived from such Confidential Information.

"Good Utility Practice" has the meaning set forth in Appendix A (the master definitions supplement) of the ISO Tariff.

"Participating Transmission Owner" has the meaning set forth in Appendix A (the master definitions supplement) of the ISO Tariff.

"Penalty" or "Penalties" means any fine, reprimand or monetary or non-monetary penalty issued or assessed by a Compliance Enforcement Authority and/or by FERC.

"Responsible Entity" means the Party that, as set forth in the CFR Matrix attached as Appendix 3 to this Agreement, has responsibility for compliance with a particular Requirement or sub-Requirement of an applicable Reliability Standard or for compliance with a particular activity or responsibility associated with that Requirement or sub-Requirement as identified in the "Responsibility Details" column of the CFR Matrix.

"Reliability Standard" means a NERC, or WECC regional, mandatory reliability standard requirement approved by the FERC under Section 215 of the Federal Power Act to provide for reliable operation of the Bulk Power System.

The terms "Each," "Single," "Split," and "Not Applicable" as used in the CFR Matrix attached to this Agreement are defined in Section 4.2 of this Agreement.

2. TERM.

2.1 Effective Date. This Agreement shall be effective as of January 1, 2015. As of the effective date, this Agreement replaces and supersedes, and operates to terminate, the prior "Reliability Standards Agreement" that the Parties executed on or about June 15, 2007.

2.2 Termination. This Agreement shall remain in effect until (1) a date upon which the Parties agree in writing to terminate it, (2) the effective date of the withdrawal of the TE's transmission facilities from the ISO Balancing Authority Area, or (3) twelve (12) months after timely written notice of termination has been provided by either Party; provided, however, that notice of termination pursuant to clause (3) herein shall be timely only if made during the Termination Window. The Termination Window shall commence on the third anniversary of the Effective Date of this Agreement, with subsequent Termination Windows commencing every two years thereafter. Each Termination Window shall be forty-five (45) calendar days in duration.

2.3 Surviving Obligations. This Agreement shall continue in effect after termination to the extent necessary to complete corrective mitigating actions identified in the Compliance monitoring process as well as satisfy all other obligations including any financial responsibilities arising under the Agreement prior to its termination. Upon termination of this Agreement, any outstanding financial right or obligation, and any provision of this Agreement necessary to give effect to such right or obligation, shall survive until satisfied.

3. PURPOSE OF AGREEMENT.

The Parties agree that the purpose of this Agreement is to identify the Parties' respective compliance responsibilities with respect to each applicable Reliability Standard and each applicable Requirement or sub-Requirement of an applicable Reliability Standard relating to the TOP function for the transmission facilities identified in Appendix 1 of this Agreement. This Agreement is limited to the Reliability Standards that are applicable to TOPs, which are identified in the CFR Matrix attached as Appendix 3, and applies only to the transmission facilities identified in Appendix 1. Each Party shall remain wholly and separately

responsible for any Reliability Standards compliance obligations that are outside the scope of this Agreement.

4. DELINEATION OF RESPONSIBILITIES BETWEEN THE ISO AND TE; CFR MATRIX.

4.1 CFR Matrix. To identify the responsibilities of each Party and to avoid gaps or redundancy in the performance of their responsibilities, the Parties have mutually collaborated in developing a CFR Matrix that identifies each Party's respective responsibilities for each Reliability Standard Requirement and sub-Requirement applicable to the ISO and the TE as TOPs registered with NERC. The Parties have determined their respective responsibilities for each such requirement based upon consideration of past practice, practicality, efficiency and Good Utility Practice. The CFR Matrix is attached as Appendix 3 to this Agreement.

4.2 Delineation of Responsibilities. The CFR Matrix sets forth the text of each Reliability Standards Requirement or sub-Requirement applicable to the TOP function and, for each such Requirement or sub-Requirement, sets forth the division of responsibility between the Parties. For each applicable Requirement or sub-Requirement, the CFR Matrix identifies the responsibility as Single, Split, Each, or Not Applicable and includes a "Responsibility Details" column that provides additional information. A "Single" designation means that only one of the Parties, as identified in the Matrix, is responsible for compliance with the specified Requirement or sub-Requirement with respect to the transmission facilities covered by the Agreement. A "Split" designation means that the Parties each have certain responsibilities with respect to the specified Requirement or sub-Requirement, which are then delineated in the Responsibility Details column. An "Each" designation means that each Party is separately and wholly responsible for compliance with the Requirement or sub-Requirement as it may pertain to that Party, though only to the extent that the Requirement or sub-Requirement pertains to that Party's activities, personnel or operations as set forth in the corresponding Responsibility Details column of the Matrix. For each of these designations, the Parties intend that, in the case of an alleged violation of a Reliability Standards Requirement or sub-Requirement, only the Party whose designated obligation has been violated should be held liable, and one Party should not be held liable for the alleged violation of a responsibility that pertains to the other Responsible Entity. A "Not Applicable" designation means that neither party has identified an applicability to their compliance obligations as a Transmission Operator for the Requirement or sub-Requirement in its entirety for the reason identified in the Responsibility Details column of the Matrix. In each instance where a Party is designated in the Matrix as having a responsibility for a particular Requirement, sub-Requirement, or portion of a Requirement or sub-Requirement, that Party holds full compliance responsibility for the

designated obligation pursuant to Rule 508 of the NERC Rules of Procedure, as it may be modified from time to time.

4.3 Process for Revising the CFR Matrix.

4.3.1 Upon approval by the FERC of any new Reliability Standard(s) or change(s) to existing Reliability Standards, the Parties shall promptly confer regarding their respective compliance responsibilities for the new or revised Standard(s) and agree upon a revision to the CFR Matrix to address the new or revised Standard(s). The Parties shall complete the revision to the CFR Matrix before the effective date of the new or revised Standard(s). The revised CFR Matrix shall replace and supersede the previous version on a going-forward basis. Such revision to the CFR Matrix does not constitute an amendment to this Agreement.

4.3.2 Upon ten (10) business days' written notice, either Party may initiate a review of the CFR Matrix for purposes of redefining the Parties' respective responsibilities for a given Requirement or sub-Requirement.

4.3.3 The Parties shall keep a mutually agreed upon revision history document that tracks each revision to the CFR Matrix, identifying the date of each revision and the change(s) made. The Parties shall also retain copies of each of the superseded versions of the CFR Matrix for reference.

5. MUTUAL COOPERATION; RESPONSE TO NOTICES OF POSSIBLE OR ALLEGED VIOLATION; ALLOCATION OF PENALTIES.

5.1 Mutual Cooperation. In addition to any obligations set forth in the CFR Matrix, the Parties agree to cooperate fully to provide each other the information, documentation and assistance necessary to demonstrate compliance with their respective obligations for the Reliability Standards requirements covered by this Agreement. This cooperation shall include, without limitation, providing each other information, documentation and assistance in connection with any audit, spot-check, investigation or inquiry brought by a Compliance Enforcement Authority or by FERC, or in connection with any self-certification or self-report, relating to one or more of the Reliability Standards requirements covered by this Agreement. Unless otherwise agreed, the Parties agree that upon fifteen (15) days of receipt of a written notice from the Party requesting the information, the other Party responsible for providing the information shall timely deliver the

requested information. The written notice shall be delivered as set forth in Section 9.18 of this Agreement, unless the Parties have agreed in writing upon an alternative person and/or means of communication.

5.2 Response to Notices of Possible or Alleged Violations. In the event that either Party receives a Notice of Possible Violation or a Notice of Alleged Violation from a Compliance Enforcement Authority or FERC with respect to one or more Reliability Standards requirements covered by this Agreement and for which the Parties' responsibility is designated as either "Not Applicable," "Split" or "Each" in the CFR Matrix, the Party receiving the notice shall notify the other Party in writing within seven (7) days of receiving the written notice. In the event that there is a disagreement between the Parties as to which of the Parties is the Responsible Entity with respect to the subject matter that is at issue in the notice, the disagreement shall be resolved in the manner set forth in Rule 508 of the NERC Rules of Procedure.

5.3 Allocation of Penalties. For any monetary Penalty imposed upon the ISO by a Compliance Enforcement Authority or FERC for a violation of any Reliability Standards Requirement or sub-Requirement covered by this Agreement, the ISO may seek authority from FERC to impose a direct or indirect allocation of the Penalty, as appropriate, through the procedure set forth in Section 14.7 of the ISO Tariff.

6. AMENDMENT TO AGREEMENT.

This Agreement may not be amended or otherwise modified without the written consent of both Parties.

7. USE OF CONTRACTORS.

Nothing in this Agreement shall prevent either the ISO or the TE from using qualified third party contractors to meet the Party's rights or obligations under this Agreement. However, under no circumstances shall the use or hiring of a qualified third party contractor or agent relieve the Responsible Entity of any liability hereunder.

8. PERFORMANCE STANDARDS.

Each Party shall perform all of its obligations under this Agreement in accordance with applicable laws and regulations, applicable Reliability Standards, and Good Utility Practice.

9. GENERAL TERMS AND CONDITIONS.

9.1 Liability. Except for Penalties assessed by a Compliance Enforcement Authority or FERC, no Party to this Agreement shall be liable to the other Party, or to any other person or entity, for any indirect, special, incidental or consequential losses, damages, claims, liabilities, costs or expenses (including attorneys' fees and court costs) arising from the performance or non-performance of its obligations under this Agreement, regardless of the cause (including intentional action, willful action, gross or ordinary negligence, or force majeure); provided, however, that a Party may seek equitable or other non-monetary relief as may be necessary to enforce this Agreement and that damages for which a Party may be liable to another Party under another agreement will not be considered damages under this Agreement. This provision also shall not limit the ISO's authority to seek approval from FERC for allocation of a monetary penalty as set forth in Section 5.3.

9.2 Confidentiality.

9.2.1 Treatment of Confidential Information. The Parties recognize and agree that for the purposes of demonstrating compliance with the Reliability Standards and preparing for a self-certification or responding to a Compliance Audit, spot-check, investigation, or inquiry by the Compliance Enforcement Authority or FERC, they may receive information from each other that has been marked as Confidential Information. Except as set forth herein, the Parties agree to keep in confidence and not to copy, disclose, or distribute to any other person or entity any Confidential Information or any part thereof provided for these evidentiary purposes, without the prior written permission of the other Party.

9.2.1.1 Location of Confidential Information. Confidential Information that the Parties have given to each other in hard copy form that is intended for disclosure to the Compliance Enforcement Authority or to FERC during the course of a Compliance Audit or other investigation or inquiry will be kept in a secure and restricted location and clearly marked so as to distinguish it from the business records of the Party receiving the Confidential Information.

9.2.1.2 Provision of Confidential Information to Compliance Enforcement Authority. During the course of a Compliance Audit or other investigation or inquiry, the Party providing the Confidential Information to the Compliance Enforcement Authority or FERC shall notify the receiving Party if and when the Compliance Enforcement Authority or FERC takes physical possession of the Confidential Information. If the Compliance Enforcement Authority or FERC takes physical possession of the Confidential Information, the receiving Party shall be permitted to make one copy of the Confidential Information that

will be afforded confidential treatment pursuant to this Agreement. To the extent the Compliance Enforcement Authority or FERC does not take physical possession of the Confidential Information, or if a copy has been made of the Confidential Information, the receiving Party shall return the Confidential Information to the providing Party promptly after the conclusion of the Compliance Audit or other applicable proceeding, including the appeal of Alleged Violations or Penalties. The Party providing the other Party's Confidential Information to the Compliance Enforcement Authority or FERC has the affirmative duty to request that the Compliance Enforcement Authority or FERC treat the Confidential Information as Confidential Information under NERC Rules of Procedure Section 1500.

9.2.2 Disclosure of Confidential Information. If, while in the possession of the receiving Party, disclosure of the Confidential Information is required to respond to a subpoena, law, or other directive of a court, administrative agency, or arbitration panel, the receiving Party hereby agrees to provide the providing Party with prompt written notice of such request or requirement in order to enable the providing Party to (a) seek an appropriate protective order or other remedy, (b) consult with the receiving Party with respect to taking steps to resist or narrow the scope of such request or legal process, or (c) waive compliance, in whole or in part, with the terms of this Section. The receiving Party agrees to work with the providing Party to obtain assurance that confidential treatment will be accorded to such Confidential Information and will cooperate to the maximum extent practicable to minimize the disclosure of the Confidential Information consistent with applicable law.

9.2.3 Exceptions to Non-Disclosure. Notwithstanding Sections 9.2.1 and 9.2.2 above, each Party to this Agreement shall not have breached any obligation under this Agreement if Confidential Information is disclosed to a third party when the Confidential Information:

(a) was in the public domain at the time of such disclosure or is subsequently made available to the public consistent with the terms of this Agreement; or

(b) had been received by either Party at the time of disclosure through other means without restriction on its use, or had been independently developed by either Party as shown through documentation; or

(c) is subsequently disclosed to either Party by a third party without restriction on use and without breach of any agreement or legal duty; or

(d) subject to the provisions of Sections 9.2.1 and 9.2.2, is used or disclosed pursuant to statutory duty or an order, subpoena or other lawful process issued by a court or other governmental authority of competent jurisdiction.

9.2.4 Other Parties. The receiving Party shall keep Confidential Information in confidence and shall not disclose such information or otherwise make it available, in any form or manner, to any other person or entity other than its employees, contractors and subcontractors as necessary for mandatory Reliability Standards compliance, without the prior written consent of the providing Party. Each Party will cause its contractors' and subcontractors' employees who will have access to Confidential Information, if any, to acknowledge that they have read and agree to abide by the terms of this Agreement regarding use and disclosure of Confidential Information.

9.3 Binding Effect. This Agreement and the rights and obligations hereof, shall be binding upon and shall inure to the benefit of the successors and assigns of the Parties hereto.

9.4 Rules of Interpretation. This Agreement, unless a clear contrary intention appears, shall be construed and interpreted as follows:

(1) the singular number includes the plural number and vice versa;

(2) reference to any person includes such person's successors and assigns but, in the case of a Party, only if such successors and assigns are permitted by this Agreement, and reference to a person in a particular capacity excludes such person in any other capacity or individually;

(3) reference to any agreement, document, instrument, or tariff means such agreement, document, instrument, or tariff as amended or modified from time to time and in effect at the time of interpretation, including, if applicable, rules and regulations promulgated thereunder;

(4) reference to any applicable laws and regulations means such applicable laws and regulations as amended, modified, codified, or reenacted, in whole or in part, and in effect at the time of interpretation, including, if applicable, rules and regulations promulgated thereunder;

(5) unless expressly stated otherwise, reference to any Article, Section, or Appendix means such Article or Section of this Agreement or such Appendix to this Agreement;

(6) “hereunder,” “hereof,” “herein,” “hereto,” and words of similar import shall be deemed references to this Agreement as a whole and not to any particular Section;

(7) “including” (and with correlative meaning “include”) means including without limiting the generality of any description preceding such term;

(8) relative to the determination of any period of time, “from” means “from and including,” “to” means “to but excluding,” and “through” means “through and including;” and

(9) “days” shall mean calendar days unless otherwise specified; if the last calendar day falls on a weekend or national holiday, the specified deadline shall fall on the next calendar day that is not a weekend or national holiday.

9.5 Entire Agreement. This Agreement, including all Attachments, Exhibits and Appendices hereto, constitutes the entire agreement between the Parties with reference to the subject matter hereof, and supersedes all prior and contemporaneous understandings or agreements, oral or written, between the Parties with respect to the subject matter of this Agreement. There are no other agreements, representations, warranties, or covenants, which constitute any part of the consideration for, or any condition to, any Party’s compliance with its obligations under this Agreement.

9.6 General Interpretation. The terms of this Agreement have been negotiated by the Parties hereto and the language used in this Agreement shall be deemed the language chosen by the Parties to express their mutual intent. This Agreement shall be construed without regard to any presumption or rule requiring construction against the party causing such instrument or portion hereof to be drafted or in favor of the party receiving a particular benefit under this Agreement. No rule of strict construction will be applied against any Party.

9.7 No Third Party Beneficiaries. This Agreement is not intended to and does not create rights, remedies, or benefits of any character whatsoever in favor of any persons, corporations, associations, or entities other than the Parties, and the obligations herein assumed are solely for the use and benefit of the Parties, their successors in interest and, where permitted, their assigns.

9.8 Waiver. The failure of a Party to this Agreement to insist, on any occasion, upon strict performance of any provision of this Agreement will not be considered a waiver of any obligation, right, or duty of, or imposed upon, such Party. Any waiver at any time by a Party of its rights with respect to this Agreement shall not be deemed a continuing waiver or a waiver with respect to

any other failure to comply with any other obligation, right, or duty of this Agreement. Any waiver of this Agreement shall, if requested, be provided in writing. Any waivers at any time by any Party of its rights with respect to any default under this Agreement, or with respect to any other matter arising in connection with this Agreement, shall not constitute or be deemed a waiver with respect to any subsequent default or other matter arising in connection with this Agreement. Any delay, short of the statutory period of limitations, in asserting or enforcing any right under this Agreement shall not constitute or be deemed a waiver of such right.

9.9 Headings. The descriptive headings of the various Articles and Sections of this Agreement have been inserted for convenience of reference only and are of no significance in the interpretation or construction of this Agreement.

9.10 Authority. The undersigned hereby represents and warrants that he or she has the requisite power and authority to bind the applicable Party to the terms and obligations of this Agreement.

9.11 Multiple Counterparts. This Agreement may be executed in two or more counterparts, each of which is deemed an original, but all constitute one and the same instrument.

9.12 No Partnership. This Agreement shall not be interpreted or construed to create an association, joint venture, agency relationship, or partnership between the Parties or to impose any partnership obligation or partnership liability upon any Party. No Party shall have any right, power or authority to enter into any agreement or undertaking for, or act on behalf of, or to act as or be an agent or representative of, or to otherwise bind, another Party.

9.13 Assignment. This Agreement may be assigned by a Party only with the written consent of the other Party; provided that a Party may assign this Agreement without the consent of the other Party to any affiliate of the assigning Party with an equal or greater credit rating and with the legal authority and operational ability to satisfy the obligations of the assigning Party under this Agreement. Any attempted assignment that violates this Section 9.13 is void and ineffective. Any assignment under this Agreement shall not relieve a Party of its obligations, nor shall a Party's obligations be enlarged, in whole or in part, by reason thereof. Where required, consent to assignment will not be unreasonably withheld, conditioned or delayed. Notwithstanding the above, this Agreement may be assigned by a governmental Party without consent of the other Parties, if the United States, a state, or a local government with jurisdiction over such Party orders such governmental Party to assign this Agreement.

9.14 Specific Performance. Each Party's obligations under this Agreement are unique. The Parties each acknowledge that, if any Party should default in performance of the duties and obligations imposed by this Agreement, it would

be extremely impracticable to measure the resulting damages. Accordingly, the non-defaulting Party, in addition to any other available rights or remedies, may seek specific performance and the Parties each expressly waive the defense that a remedy in damages will be adequate.

9.15 Force Majeure. No Party shall be liable for any failure to perform its obligations in connection with any action described in this Agreement, if such failure results from an Uncontrollable Force as defined in the ISO Tariff (including any mechanical, electronic, or communication failures, but excluding failure caused by a party's financial condition or negligence).

9.16 Governing Law. The rights and obligations of the Parties and the interpretation and performance of this Agreement shall be governed by the law of California, excluding its conflicts of law rules, except if a federal Party is involved, in which case federal law shall apply as if performed within the state of California. Notwithstanding the foregoing, nothing shall affect the rights of the Parties under the Federal Power Act, any applicable agreement, the NERC Rules of Procedure, or rules or orders promulgated by FERC.

9.17 Consistency with Federal Laws and Regulations. Section 22.9 of the ISO Tariff titled "Consistency with Federal Laws and Regulations" is hereby incorporated herein by reference, providing however, that the references to the ISO Tariff in Section 22.9 shall include this Agreement.

9.18 Notices. Any written notice provided for in this Agreement shall be in writing transmitted via electronic mail to the persons identified in Appendix 2, followed with a hard copy delivered in person or sent by overnight mail or United States certified mail within three (3) days of the electronic mail transmission. Electronic mail notice shall be deemed effective upon transmission unless the Party sending the electronic mail learns that delivery was unsuccessful, in which case notice is deemed effective upon service of the hard copy. Any Party may at any time, by at least fifteen (15) days notice to the other Party, change the designation or address of a person specified in Appendix 2. Such a change to Appendix 2 shall not constitute an amendment to this Agreement.

9.19 FERC Jurisdiction. Nothing in this Agreement shall be meant to imply or cede jurisdiction to FERC, NERC or any other regulatory or Compliance Enforcement Authority, to the extent that FERC, NERC or other regulatory or Compliance Enforcement Authority does not have jurisdiction over a Party to this Agreement. FERC, NERC and other regulatory or Compliance Enforcement Authority entities have limited jurisdiction over certain Parties and, by executing this Agreement, no Party is waiving or conceding any defenses it has to assert jurisdictional defenses, including, but not limited to, sovereign immunity, intergovernmental immunities, or lack of subject matter jurisdiction.

9.20 Severability. If any term or provision of this Agreement is held to be illegal, invalid, or unenforceable under any present or future law or by FERC, (a) such term or provision shall be fully severable, (b) this Agreement shall be construed and enforced as if such illegal, invalid or unenforceable provision had never comprised a part hereof, and (c) the remaining provisions of this Agreement shall remain in full force and effect and shall not be affected by the illegal, invalid or unenforceable provision or by its severance herefrom.

IN WITNESS WHEREOF, the Parties have executed this Agreement and it is effective as of the effective date pursuant to Section 2.1.

California Independent System Operator Corporation

By: _____

Name: **Eric J. Schmitt**

Title: **Vice President, Operations**

Date: 10/21/14

Pacific Gas and Electric Company

By: _____

Name: Gregg Lemler

Title: Vice President, Transmission Operations

Date: 12-9-2014

APPENDIX 1

APPLICABLE TRANSMISSION FACILITIES

The transmission facilities subject to the terms of this Agreement include all PG&E-owned transmission facilities entered into the ISO Register that are designated as subject to the control of the ISO, as the ISO Register is amended or modified, in whole or in part, from time to time.

APPENDIX 2

Pacific Gas and Electric Company

Name of Primary Representative:	Roderick Robinson
Title:	VP, Electric System Operations
Company:	Pacific Gas and Electric Company
Address:	4940 Allison Parkway
City / State / Zip Code:	Vacaville, CA 95688
Email Address:	Roderick.Robinson@pge.com
Telephone:	707-449-6610

Name of Alternative Representative:	Ahmad Ababneh
Title:	VP, Transmission & Substation Operations
Company:	Pacific Gas and Electric Company
Address:	300 Lakeside Drive
City / State / Zip Code:	Oakland, CA 94612
Email Address:	Ahmad.Ababneh@pge.com
Telephone:	415-969-0958

ISO

Name of Primary Representative:	Lisa Milanes
Title:	Director, Corporate Compliance
Address:	250 Outcropping Way
City/State/Zip Code:	Folsom, CA 95630
Email address:	lmilanes@caiso.com
Phone:	(916) 351-2172
Fax:	(916) 608-7222

Name of Alternative Representative:	Burton Gross
Title:	Assistant General Counsel
Address:	250 Outcropping Way
City/State/Zip Code:	Folsom, CA 95630
Email address:	bgross@caiso.com
Phone:	(916) 608-7268
Fax:	(916) 608-7222

APPENDIX 3

CFR Matrix

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-002-5.1a	R1	Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: i.Control Centers and backup Control Centers; ii.Transmission stations and substations; iii.Generation resources; iv.Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements; v.Special Protection Systems that support the reliable operation of the Bulk Electric System; and vi.For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-002-5.1a	R1.1	Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-002-5.1a	R1.2	Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-002-5.1a	R1.3	Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-002-5.1a	R2	The Responsible Entity shall:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-002-5.1a	R2.1	Review the identifications in Requirement R1 and its parts (and update them if there are changes identified) at least once every 15 calendar months, even if it has no identified items in Requirement R1, and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-002-5.1a	R2.2	Have its CIP Senior Manager or delegate approve the identifications required by Requirement R1 at least once every 15 calendar months, even if it has no identified items in Requirement R1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.	Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.	For its high impact and medium impact BES Cyber Systems, if any:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-003-9	R1.1.1.	Personnel and training (CIP-004);	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.2.	Electronic Security Perimeters (CIP-005) including Interactive Remote Access;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.3.	Physical security of BES Cyber Systems (CIP-006);	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.4.	System security management (CIP-007);	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.5.	Incident reporting and response planning (CIP-008);	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.6.	Recovery plans for BES Cyber Systems (CIP-009);	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.7.	Configuration change management and vulnerability assessments (CIP-010);	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.8.	Information protection (CIP-011); and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.1.9.	Declaring and responding to CIP Exceptional Circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.	For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.1.	Cyber security awareness;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.2.	Physical security controls;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.3.	Electronic access controls;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.4.	Cyber Security Incident response;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.5.	Transient Cyber Assets and Removable Media malicious code risk mitigation; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-003-9	R1.2.6.	Vendor electronic remote access security controls; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R1.2.7	Declaring and responding to CIP Exceptional Circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R2.	Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cyber security plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R3.	Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-003-9	R4.	The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R1.	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-004-7 Table R1 – Security Awareness Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R1.1.	Security awareness that, at least once each calendar quarter, reinforces cyber security practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.	Each Responsible Entity shall implement one or more cyber security training program(s) appropriate to individual roles, functions, or responsibilities that collectively includes each of the applicable requirement parts in CIP-004-7 Table R2 – Cyber Security Training Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-004-7	R2.1.	Training content on:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.1.	Cyber security policies;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.2.	Physical access controls;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.3.	Electronic access controls;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.4.	The visitor control program;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.5.	Handling of BES Cyber System Information and its storage;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.6.	Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.7.	Recovery plans for BES Cyber Systems;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.8.	Response to Cyber Security Incidents; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.1.9.	Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including Transient Cyber Assets, and with Removable Media.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.2.	Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R2.3.	Require completion of the training specified in Part 2.1 at least once every 15 calendar months.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-004-7	R3.	Each Responsible Entity shall implement one or more documented personnel risk assessment program(s) to attain and retain authorized electronic or authorized unescorted physical access to BES Cyber Systems that collectively include each of the applicable requirement parts in CIP-004-7 Table R3 – Personnel Risk Assessment Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.1.	Process to confirm identity.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.2.	Process to perform a seven year criminal history records check as part of each personnel risk assessment that includes:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.3.	Criteria or process to evaluate criminal history records checks for authorizing access.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.4.	Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.5.	Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.2.1.	current residence, regardless of duration; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R3.2.2.	other locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has resided for six consecutive months or more. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-004-7	R4.	Each Responsible Entity shall implement one or more documented access management program(s) that collectively include each of the applicable requirement parts in CIP-004-7 Table R4 – Access Management Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R4.1.	Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R4.1.2.	Unescorted physical access into a Physical Security Perimeter	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R4.1.1.	Electronic access; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R4.2.	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R4.3.	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R5.	Each Responsible Entity shall implement one or more documented access revocation program(s) that collectively include each of the applicable requirement parts in CIP-004-7 Table R5 – Access Revocation.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R5.1.	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R5.2.	For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-004-7	R5.3.	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Part 5.1) within 30 calendar days of the effective date of the termination action.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R5.4.	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.	Each Responsible Entity shall implement one or more documented access management program(s) to authorize, verify, and revoke provisioned access to BCSI pertaining to the "Applicable Systems" identified in CIP-004-7 Table R6 – Access Management for BES Cyber System Information that collectively include each of the applicable requirement parts in CIP-004-X Table R6 – Access Management for BES Cyber System Information. To be considered access to BCSI in the context of this requirement, an individual has both the ability to obtain and use BCSI. Provisioned access is to be considered the result of the specific actions taken to provide an individual(s) the means to access BCSI (e.g., may include physical keys or access cards, user accounts and associated rights and privileges, encryption keys).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.1.	Prior to provisioning, authorize (unless already authorized according to Part 4.1.) based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.2.	Verify at least once every 15 calendar months that all individuals with provisioned access to BCSI:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-004-7	R6.3.	For termination actions, remove the individual's ability to use provisioned access to BCSI (unless already revoked according to Part 5.1) by the end of the next calendar day following the effective date of the termination action.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.1.1.	Provisioned electronic access to electronic BCSI; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.1.2.	Provisioned physical access to physical BCSI.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.2.1.	have an authorization record; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-004-7	R6.2.2.	still need the provisioned access to perform their current work functions, as determined by the Responsible Entity.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R1.	Each Responsible Entity shall implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-005-7 Table R1 – Electronic Security Perimeter.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R1.1.	All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R1.2.	All External Routable Connectivity must be through an identified Electronic Access Point (EAP).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R1.3.	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R1.4.	Where technically feasible, perform authentication when establishing Dial-up Connectivity with applicable Cyber Assets.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R1.5.	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R2.	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts, where technically feasible, in CIP-005-7 Table R2 –Remote Access Management.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R2.1.	For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-005-7	R2.2.	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R2.3.	Require multi-factor authentication for all Interactive Remote Access sessions.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R2.4.	Have one or more methods for determining active vendor remote access sessions (including Interactive Remote Access and system-to-system remote access).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R2.5.	Have one or more method(s) to disable active vendor remote access including Interactive Remote Access and system-to-system remote access).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R3.	Each Responsible Entity shall implement one or more documented processes that collectively include the applicable requirement parts in CIP-005-7 Table R3 –Vendor Remote Access Management for EACMS and PACS.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R3.1.	Have one or more method(s) to determine authenticated vendor-initiated remote connections.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-005-7	R3.2.	Have one or more method(s) to terminate authenticated vendor-initiated remote connections and control the ability to reconnect.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1	Each Responsible Entity shall implement one or more documented physical security plan(s) that collectively include all of the applicable requirement parts in CIP-006-6 Table R1 – Physical Security Plan.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.1	Define operational or procedural controls to restrict physical access.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.2	Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.3	Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-006-6	R1.4	Monitor for unauthorized access through a physical access point into a Physical Security Perimeter.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.5	Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.6	Monitor each Physical Access Control System for unauthorized physical access to a Physical Access Control System.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.7	Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.8	Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R1.9	Retain physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-006-6	R1.10	Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. Where physical access restrictions to such cabling and components are not implemented, the Responsible Entity shall document and implement one or more of the following: - encryption of data that transits such cabling and components; or - monitoring the status of the communication link composed of such cabling and components and issuing an alarm or alert in response to detected communication failures to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of detection; or - an equally effective logical protection.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R2	Each Responsible Entity shall implement one or more documented visitor control program(s) that include each of the applicable requirement parts in CIP-006-6 Table R2 – Visitor Control Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R2.1	Require continuous escorted access of visitors (individuals who are provided access but are not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R2.2	Require manual or automated logging of visitor entry into and exit from the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor's name, and the name of an individual point of contact responsible for the visitor, except during CIP Exceptional Circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R2.3	Retain visitor logs for at least ninety calendar days.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-006-6	R3	Each Responsible Entity shall implement one or more documented Physical Access Control System maintenance and testing program(s) that collectively include each of the applicable requirement parts in CIP-006-6 Table R3 – Maintenance and Testing Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-006-6	R3.1	Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R1	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R1 – Ports and Services.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R1.2	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or Removable Media.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R2	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R2 – Security Patch Management.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R2.2	At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-007-6	R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: - Apply the applicable patches; or - Create a dated mitigation plan; or - Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R2.4	For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R3	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R3.1	Deploy method(s) to deter, detect, or prevent malicious code.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R3.2	Mitigate the threat of detected malicious code.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R3.3	For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R4 – Security Event Monitoring.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.1	Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-007-6	R4.1.1	Detected successful login attempts;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.1.2	Detected failed access attempts and failed login attempts;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.1.3	Detected malicious code.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.2	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.2.1	Detected malicious code from Part 4.1; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.2.2	Detected failure of Part 4.1 event logging.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R5 – System Access Controls.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.3	Identify individuals who have authorized access to shared accounts.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.4	Change known default passwords, per Cyber Asset capability	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-007-6	R5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.5.1	Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.5.2	Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-007-6	R5.7	Where technically feasible, either: - Limit the number of unsuccessful authentication attempts; or - Generate alerts after a threshold of unsuccessful authentication attempts.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1	Each Responsible Entity shall document one or more Cyber Security Incident response plan(s) that collectively include each of the applicable requirement parts in CIP-008-6 Table R1 – Cyber Security Incident Response Plan Specifications.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1.1	One or more processes to identify, classify, and respond to Cyber Security Incidents.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1.2	One or more processes:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1.2.1	That include criteria to evaluate and define attempts to compromise;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1.2.2	To determine if an identified Cyber Security Incident is: • A Reportable Cyber Security Incident; or • An attempt to compromise, as determined by applying the criteria from Part 1.2.1, one or more systems identified in the "Applicable Systems" column for this Part; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1.2.3	To provide notification per Requirement R4.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-008-6	R1.3	The roles and responsibilities of Cyber Security Incident response groups or individuals.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R1.4	Incident handling procedures for Cyber Security Incidents.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R2	Each Responsible Entity shall implement each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R2.1	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: - By responding to an actual Reportable Cyber Security Incident; - With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or - With an operational exercise of a Reportable Cyber Security Incident.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R2.2	Use the Cyber Security Incident response plan(s) under Requirement R1 when responding to a Reportable Cyber Security Incident, responding to a Cyber Security Incident that attempted to compromise a system identified in the "Applicable Systems" column for this Part, or performing an exercise of a Reportable Cyber Security Incident. Document deviations from the plan(s) taken during the response to the incident or exercise.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R2.3	Retain records related to Reportable Cyber Security Incidents and Cyber Security Incidents that attempted to compromise a system identified in the "Applicable Systems" column for this Part as per the Cyber Security Incident response plan(s) under Requirement R1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3	Each Responsible Entity shall maintain each of its Cyber Security Incident response plans according to each of the applicable requirement parts in CIP-008-6 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-008-6	R3.1	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3.1.1	Document any lessons learned or document the absence of any lessons learned;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3.1.2	Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3.1.3	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, Cyber Security Incident response groups or individuals, or technology that the Responsible Entity determines would impact the ability to execute the plan:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3.2.1	Update the Cyber Security Incident response plan(s); and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R3.2.2	Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R4	Each Responsible Entity shall notify the Electricity Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC), 1 or their successors, of a Reportable Cyber Security Incident and a Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-6 Table R4 – Notifications and Reporting for Cyber Security Incidents.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R4.1	Initial notifications and updates shall include the following attributes, at a minimum, to the extent known:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-008-6	R4.1.1	4.1.1 The functional impact;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R4.1.2	4.1.2 The attack vector used; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R4.1.3	4.1.3 The level of intrusion that was achieved or attempted.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R4.2	After the Responsible Entity's determination made pursuant to documented process(es) in Requirement R1, Part 1.2, provide initial notification within the following timelines: • One hour after the determination of a Reportable Cyber Security Incident. • By the end of the next calendar day after determination that a Cyber Security Incident was an attempt to compromise a system identified in the "Applicable System	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-008-6	R4.3	Provide updates, if any, within 7 calendar days of determination of new or changed attribute information required in Part 4.1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R1	Each Responsible Entity shall have one or more documented recovery plan(s) that collectively include each of the applicable requirement parts in CIP-009-6 Table R1 – Recovery Plan Specifications.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R1.1	Conditions for activation of the recovery plan(s).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R1.2	Roles and responsibilities of responders.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R1.3	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R1.4	One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R1.5	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-009-6	R2	Each Responsible Entity shall implement its documented recovery plan(s) to collectively include each of the applicable requirement parts in CIP-009-6 Table R2 – Recovery Plan Implementation and Testing.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R2.1	Test each of the recovery plans referenced in Requirement R1 at least once every 15 calendar months: - By recovering from an actual incident; - With a paper drill or tabletop exercise; or - With an operational exercise.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R2.2	Test a representative sample of information used to recover BES Cyber System functionality at least once every 15 calendar months to ensure that the information is useable and is compatible with current configurations. An actual recovery that incorporates the information used to recover BES Cyber System functionality substitutes for this test.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R2.3	Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3	Each Responsible Entity shall maintain each of its recovery plan(s) in accordance with each of the applicable requirement parts in CIP-009-6 Table R3 – Recovery Plan Review, Update and Communication.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3.1	No later than 90 calendar days after completion of a recovery plan test or actual recovery:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3.1.1	Document any lessons learned associated with a recovery plan test or actual recovery or document the absence of any lessons learned;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3.1.2	Update the recovery plan based on any documented lessons learned associated with the plan; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3.1.3	Notify each person or group with a defined role in the recovery plan of the updates to the recovery plan based on any documented lessons learned.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-009-6	R3.2	No later than 60 calendar days after a change to the roles or responsibilities, responders, or technology that the Responsible Entity determines would impact the ability to execute the recovery plan:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3.2.1	Update the recovery plan; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-009-6	R3.2.2	Notify each person or group with a defined role in the recovery plan of the updates.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.	R1. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4 Table R1 – Configuration Change Management.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.1.	Develop a baseline configuration, individually or by group, which shall include the following items:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.1.1.	Operating system(s) (including version) or firmware where no independent operating system exists;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.1.2.	Any commercially available or open-source application software (including version) intentionally installed;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.1.3.	Any custom software installed;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.1.4.	Any logical network accessible ports; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.1.5.	Any security patches applied.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.2.	Authorize and document changes that deviate from the existing baseline configuration.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.3.	For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.4.	For a change that deviates from the existing baseline configuration:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-010-4	R1.4.1.	Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.4.2.	Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.4.3.	Document the results of the verification.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.5.	Where technically feasible, for each change that deviates from the existing baseline configuration:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.5.1.	Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.5.2.	Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.6.	Prior to a change that deviates from the existing baseline configuration associated with baseline items in Parts 1.1.1, 1.1.2, and 1.1.5, and when the method to do so is available to the Responsible Entity from the software source:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.6.1.	Verify the identity of the software source; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R1.6.2.	Verify the integrity of the software obtained from the software source.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-4 Table R2 – Configuration Monitoring	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-010-4	R2.1.	Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.	Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-010-3 Table R3– Vulnerability Assessments.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.1.	At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.2.	Where technically feasible, at least once every 36 calendar months:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.2.1.	Perform an active vulnerability assessment in a test environment, or perform an active vulnerability assessment in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration of the BES Cyber System in a production environment; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.2.2.	Document the results of the testing and, if a test environment was used, the differences between the test environment and the production environment, including a description of the measures used to account for any differences in operation between the test and production environments.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.3.	Prior to adding a new applicable Cyber Asset to a production environment, perform an active vulnerability assessment of the new Cyber Asset, except for CIP Exceptional Circumstances and like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing Cyber Asset	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-010-4	R3.4.	Document the results of the assessments conducted according to Parts 3.1, 3.2, and 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-010-4	R4.	Each Responsible Entity, for its high impact and medium impact BES Cyber Systems and associated Protected Cyber Assets, shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) for Transient Cyber Assets and Removable Media that include the sections in Attachment 1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-011-3	R1.	Each Responsible Entity shall implement one or more documented information protection program(s) for BES Cyber System Information (BCSI) pertaining to "Applicable Systems" identified in CIP-011-3 Table R1 – Information Protection Program that collectively includes each of the applicable requirement parts in CIP-011-3 Table R1 – Information Protection Program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-011-3	R1.1.	Method(s) to identify BCSI.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-011-3	R1.2.	Method(s) to protect and securely handle BCSI to mitigate risks of compromising confidentiality.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-011-3	R2.	Each Responsible Entity shall implement one or more documented process(es) that collectively include the applicable requirement parts in CIP-011-3 Table R2 – BES Cyber Asset Reuse and Disposal.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-011-3	R2.1.	Prior to the release for reuse of applicable Cyber Assets that contain BCSI (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset data storage media.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-011-3	R2.2.	Prior to the disposal of applicable Cyber Assets that contain BCSI, the Responsible Entity shall take action to prevent the unauthorized retrieval of BCSI from the Cyber Asset or destroy the data storage media.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-012-1	R1.	The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-012-1	R1.1.	Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-012-1	R1.2.	Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-012-1	R1.3.	If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.	Each Responsible Entity shall develop one or more documented supply chain cyber security risk management plan(s) for high and medium impact BES Cyber Systems and their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). The plan(s) shall include:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.1.	One or more process(es) used in planning for the procurement of BES Cyber Systems and their associated EACMS and PACS to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s).	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.2.	One or more process(es) used in procuring BES Cyber Systems, and their associated EACMS and PACS, that address the following, as applicable:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-013-2	R1.2.1.	Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.2.2.	Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to the Responsible Entity;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.2.3.	Notification by vendors when remote or onsite access should no longer be granted to vendor representatives;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.2.4.	Disclosure by vendors of known vulnerabilities related to the products or services provided to the Responsible Entity;	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.2.5.	Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System and their associated EACMS and PACS; and	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R1.2.6.	Coordination of controls for vendor-initiated remote access.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R2.	Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-013-2	R3.	Each Responsible Entity shall review and obtain CIP Senior Manager or delegate approval of its supply chain cyber security risk management plan(s) specified in Requirement R1 at least once every 15 calendar months.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this Standard Requirement for their respective facilities
CIP-014-3	R4.	Each Transmission Owner that identified a Transmission station, Transmission substation, or a primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack to each of their respective Transmission station(s), Transmission substation(s), and primary control center(s) identified in Requirement R1 and verified according to Requirement R2. The evaluation shall consider the following:		X	Single	
CIP-014-3	R4.1.	Unique characteristics of the identified and verified Transmission station(s), Transmission substation(s), and primary control center(s);		X	Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-014-3	R4.2.	Prior history of attack on similar facilities taking into account the frequency, geographic proximity, and severity of past physical security related events; and		X	Single	
CIP-014-3	R4.3.	Intelligence or threat warnings received from sources such as law enforcement, the Electric Reliability Organization (ERO), the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), U.S. federal and/or Canadian governmental agencies, or their successors.		X	Single	
CIP-014-3	R5.	Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall develop and implement a documented physical security plan(s) that covers their respective Transmission station(s), Transmission substation(s), and primary control center(s). The physical security plan(s) shall be developed within 120 calendar days following the completion of Requirement R2 and executed according to the timeline specified in the physical security plan(s). The physical security plan(s) shall include the following attributes:		X	Single	
CIP-014-3	R5.1.	Resiliency or security measures designed collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4.		X	Single	
CIP-014-3	R5.2.	Law enforcement contact and coordination information.		X	Single	
CIP-014-3	R5.3.	A timeline for executing the physical security enhancements and modifications specified in the physical security plan.		X	Single	
CIP-014-3	R5.4.	Provisions to evaluate evolving physical threats, and their corresponding security measures, to the Transmission station(s), Transmission substation(s), or primary control center(s).		X	Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-014-3	R6.	Each Transmission Owner that identified a Transmission station, Transmission substation, or primary control center in Requirement R1 and verified according to Requirement R2, and each Transmission Operator notified by a Transmission Owner according to Requirement R3, shall have an unaffiliated third party review the evaluation performed under Requirement R4 and the security plan(s) developed under Requirement R5. The review may occur concurrently with or after completion of the evaluation performed under Requirement R4 and the security plan development under Requirement R5.		X	Single	
CIP-014-3	R6.1.	Each Transmission Owner and Transmission Operator shall select an unaffiliated third party reviewer from the following: - An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification. - An entity or organization approved by the ERO. - A governmental agency with physical security expertise. - An entity or organization with demonstrated law enforcement, government, or military physical security expertise.		X	Single	
CIP-014-3	R6.2.	The Transmission Owner or Transmission Operator, respectively, shall ensure that the unaffiliated third party review is completed within 90 calendar days of completing the security plan(s) developed in Requirement R5. The unaffiliated third party review may, but is not required to, include recommended changes to the evaluation performed under Requirement R4 or the security plan(s) developed under Requirement R5.		X	Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
CIP-014-3	R6.3.	If the unaffiliated third party reviewer recommends changes to the evaluation performed under Requirement R4 or security plan(s) developed under Requirement R5, the Transmission Owner or Transmission Operator shall, within 60 calendar days of the completion of the unaffiliated third party review, for each recommendation: - Modify its evaluation or security plan(s) consistent with the recommendation; or - Document the reason(s) for not modifying the evaluation or security plan(s) consistent with the recommendation.		X	Single	
CIP-014-3	R6.4.	Each Transmission Owner and Transmission Operator shall implement procedures, such as the use of non-disclosure agreements, for protecting sensitive or confidential information made available to the unaffiliated third party reviewer and to protect or exempt sensitive or confidential information developed pursuant to this Reliability Standard from public disclosure.		X	Single	
COM-001-3	R3.	Each Transmission Operator shall have Interpersonal Communication capability with the following entities (unless the Transmission Operator detects a failure of its Interpersonal Communication capability in which case Requirement R10 shall apply):	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R3.1.	Its Reliability Coordinator.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R3.2.	Each Balancing Authority within its Transmission Operator Area.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R3.3.	Each Distribution Provider within its Transmission Operator Area.		X	Single	
COM-001-3	R3.4.	Each Generator Operator within its Transmission Operator Area.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R3.5.	Each adjacent Transmission Operator synchronously connected.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
COM-001-3	R3.6.	Each adjacent Transmission Operator asynchronously connected.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R4.	Each Transmission Operator shall designate an Alternative Interpersonal Communication capability with the following entities:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R4.1.	Its Reliability Coordinator.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R4.2.	Each Balancing Authority within its Transmission Operator Area.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R4.3.	Each adjacent Transmission Operator synchronously connected.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R4.4.	Each adjacent Transmission Operator asynchronously connected.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R9.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall test its Alternative Interpersonal Communication capability at least once each calendar month. If the test is unsuccessful, the responsible entity shall initiate action to repair or designate a replacement Alternative Interpersonal Communication capability within 2 hours.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-001-3	R10.	Each Reliability Coordinator, Transmission Operator, and Balancing Authority shall notify entities as identified in Requirements R1, R3, and R5, respectively within 60 minutes of the detection of a failure of its Interpersonal Communication capability that lasts 30 minutes or longer.	X	X	Split	The CAISO and the TE shall each separately maintain compliance with this requirement as it applies to the detection of a failure of their respective Interpersonal Communication capabilities with the RC, BA, GOPs and TOPs within its TOP area. (R3.1, R3.2, R3.4 - R3.6) The TE shall maintain compliance with this requirement as it applies to each Distribution Provider in its TOP area. (R3.3)

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
COM-001-3	R12.	Each Reliability Coordinator, Transmission Operator, Generator Operator, and Balancing Authority shall have internal Interpersonal Communication capabilities for the exchange of information necessary for the Reliable Operation of the BES. This includes communication capabilities between Control Centers within the same functional entity, and/or between a Control Center and field personnel.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Interpersonal Communication capabilities.
COM-002-4	R1	Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall develop documented communications protocols for its operating personnel that issue and receive Operating Instructions. The protocols shall, at a minimum:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R1.1	Require its operating personnel that issue and receive an oral or written Operating Instruction to use the English language, unless agreed to otherwise. An alternate language may be used for internal operations.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R1.2	Require its operating personnel that issue an oral two-party, person-to-person Operating Instruction to take one of the following actions: - Confirm the receiver's response if the repeated information is correct. - Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver. - Take an alternative action if a response is not received or if the Operating Instruction was not understood by the receiver.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R1.3	Require its operating personnel that receive an oral two-party, person-to-person Operating Instruction to take one of the following actions: - Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct. - Request that the issuer reissue the Operating Instruction.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R1.4	Require its operating personnel that issue a written or oral single-party to multiple-party burst Operating Instruction to confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
COM-002-4	R1.5	Specify the instances that require time identification when issuing an oral or written Operating Instruction and the format for that time identification.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R1.6	Specify the nomenclature for Transmission interface Elements and Transmission interface Facilities when issuing an oral or written Operating Instruction.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R2	Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall conduct initial training for each of its operating personnel responsible for the Real-time operation of the interconnected Bulk Electric System on the documented communications protocols developed in Requirement R1 prior to that individual operator issuing an Operating Instruction.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
COM-002-4	R4	Each Balancing Authority, Reliability Coordinator, and Transmission Operator shall at least once every twelve (12) calendar months	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R4.1	Assess adherence to the documented communications protocols in Requirement R1 by its operating personnel that issue and receive Operating Instructions, provide feedback to those operating personnel and take corrective action, as deemed appropriate by the entity, to address deviations from the documented protocols.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols
COM-002-4	R4.2	Assess the effectiveness of its documented communications protocols in Requirement R1 for its operating personnel that issue and receive Operating Instructions and modify its documented communication protocols, as necessary.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective communications protocols

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
COM-002-4	R5	Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: - Confirm the receiver's response if the repeated information is correct (in accordance with Requirement R6). - Reissue the Operating Instruction if the repeated information is incorrect or if requested by the receiver, or - Take an alternative action if a response is not received or if the Operating Instruction was not understood by the receiver.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
COM-002-4	R6	Each Balancing Authority, Distribution Provider, Generator Operator, and Transmission Operator that receives an oral two-party, person-to-person Operating Instruction during an Emergency, excluding written or oral single-party to multiple-party burst Operating Instructions, shall either: - Repeat, not necessarily verbatim, the Operating Instruction and receive confirmation from the issuer that the response was correct, or - Request that the issuer reissue the Operating Instruction.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
COM-002-4	R7	Each Balancing Authority, Reliability Coordinator, and Transmission Operator that issues a written or oral single-party to multiple-party burst Operating Instruction during an Emergency shall confirm or verify that the Operating Instruction was received by at least one receiver of the Operating Instruction	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
EOP-004-4	R1.	Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-4 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the Regional Entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority).	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-004-4	R2	Each Responsible Entity shall report events specified in EOP-004-4 Attachment 1 to the entities specified per their event reporting Operating Plan by the later of 24 hours of recognition of meeting an event type threshold for reporting or by the end of the Responsible Entity's next business day (4 p.m. local time will be considered the end of the business day).	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
EOP-005-3	R1.	Each Transmission Operator shall develop and implement a restoration plan approved by its Reliability Coordinator. The restoration plan shall be implemented to restore the Transmission Operator's System following a Disturbance in which one or more areas of the Bulk Electric System (BES) shuts down and the use of Blackstart Resources is required to restore the shutdown area to a state whereby the choice of the next Load to be restored is not driven by the need to control frequency or voltage regardless of whether the Blackstart Resource is located within the Transmission Operator's System. The restoration plan shall include:	X	X	Each	The CAISO and TE will each have a Restoration Plan as set forth in R1. The CAISO and the TE's restoration plans shall include, to the extent applicable, the R1 sub-requirements as detailed below.
EOP-005-3	R1.1	Strategies for System restoration that are coordinated with its Reliability Coordinator's high level strategy for restoring the Interconnection.	X		Single	
EOP-005-3	R1.2	A description of how all Agreements or mutually-agreed upon procedures or protocols for off-site power requirements of nuclear power plants, including priority of restoration, will be fulfilled during System restoration.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R1.3	Procedures for restoring interconnections with other Transmission Operators under the direction of its Reliability Coordinator.	X		Single	
EOP-005-3	R1.4	Identification of each Blackstart Resource and its characteristics including but not limited to the following: the name of the Blackstart Resource, location, megawatt and megavar capacity, and type of unit.	X		Single	
EOP-005-3	R1.5	Identification of Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.		X	Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-005-3	R1.6	Identification of acceptable operating voltage and frequency limits during restoration.	X	X	Split	The CAISO will identify acceptable frequency limits to be used during restoration. The TE will identify acceptable voltage limits to be used during restoration.
EOP-005-3	R1.7	Operating Processes to reestablish connections within the Transmission Operator's System for areas that have been restored and are prepared for reconnection.	X		Single	
EOP-005-3	R1.8	Operating Processes to restore Loads required to restore the System, such as station service for substations, units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control.	X	X	Split	The CAISO shall identify loads required to restore the System, such as units to be restarted or stabilized, the Load needed to stabilize generation and frequency, and provide voltage control. The TE shall identify station service loads required to restore the System.
EOP-005-3	R1.9	Operating Processes for transferring authority back to the Balancing Authority in accordance with its Reliability Coordinator's criteria.	X		Single	
EOP-005-3	R2	Each Transmission Operator shall provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the effective date of the plan.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R3	Each Transmission Operator shall review its restoration plan and submit it to its Reliability Coordinator annually on a mutually-agreed, predetermined schedule.	X	X	Split	The CAISO and TE shall each review their restoration plans. The CAISO will submit the TE's restoration plan and the CAISO's overarching plan to the RC.
EOP-005-3	R4	Each Transmission Operator shall submit its revised restoration plan to its Reliability Coordinator for approval, when the revision would change its ability to implement its restoration plan, as follows:	X	X	Split	The CAISO and TE shall each revise their restoration plans in accordance with this requirement. The CAISO will submit the TE's revised restoration plan and the CAISO's revised overarching plan to the RC.
EOP-005-3	R4.1	Within 90 calendar days after identifying any unplanned permanent BES modifications.	X	X	Split	The CAISO and TE shall each revise their restoration plans in accordance with this requirement. The CAISO will submit the TE's revised restoration plan and the CAISO's revised overarching plan to the RC.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-005-3	R4.2.	Prior to implementing a planned permanent BES modification subject to its Reliability Coordinator approval requirements per EOP-006.	X	X	Split	The CAISO and TE shall each revise their restoration plans in accordance with this requirement. The CAISO will submit the TE's revised restoration plan and the CAISO's revised overarching plan to the RC.
EOP-005-3	R5	Each Transmission Operator shall have a copy of its latest Reliability Coordinator approved restoration plan within its primary and backup control rooms so that it is available to all of its System Operators prior to its effective date.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective control rooms.
EOP-005-3	R6	Each Transmission Operator shall verify through analysis of actual events, a combination of steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed at least once every five years. Such analysis, simulations or testing shall verify:	X		Single	
EOP-005-3	R6.1	The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.	X		Single	
EOP-005-3	R6.2	The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.	X		Single	
EOP-005-3	R6.3	The capability of generating resources required to control voltages and frequency within acceptable operating limits.	X		Single	
EOP-005-3	R7	Each Transmission Operator shall have Blackstart Resource testing requirements to verify that each Blackstart Resource is capable of meeting the requirements of its restoration plan. These Blackstart Resource testing requirements shall include:	X		Single	
EOP-005-3	R7.1.	The frequency of testing such that each Blackstart Resource is tested at least once every three calendar years.	X		Single	
EOP-005-3	R7.2.	A list of required tests including:	X		Single	
EOP-005-3	R7.2.1.	The ability to start the unit when isolated with no support from the BES or when designed to remain energized without connection to the remainder of the System.	X		Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-005-3	R7.2.2.	The ability to energize a bus. If it is not possible to energize a bus during the test, the testing entity must affirm that the unit has the capability to energize a bus such as verifying that the breaker close coil relay can be energized with the voltage and frequency monitor controls disconnected from the synchronizing circuits.	X		Single	
EOP-005-3	R7.3.	The minimum duration of each of the required tests.	X		Single	
EOP-005-3	R8	Each Transmission Operator shall include within its operations training program, annual System restoration training for its System Operators. This training program shall include training on the following:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R8.1.	System restoration plan including coordination with its Reliability Coordinator and Generator Operators included in the restoration plan.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans. The TE's training shall include training on coordination with the CAISO, rather than with the RC and with Generator Operators.
EOP-005-3	R8.2.	Restoration priorities.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R8.3.	Building of cranking paths.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R8.4.	Synchronizing (re-energized sections of the System).	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R8.5.	Transition of Demand and resource balance within its area to the Balancing Authority.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective restoration plans.
EOP-005-3	R9	Each Transmission Operator, each applicable Transmission Owner, and each applicable Distribution Provider shall provide a minimum of two hours of System restoration training every two calendar years to their field switching personnel identified as performing unique tasks associated with the Transmission Operator's restoration plan that are outside of their normal tasks.		X	Single	
EOP-005-3	R10	Each Transmission Operator shall participate in its Reliability Coordinator's restoration drills, exercises, or simulations as requested by its Reliability Coordinator.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-005-3	R11.	Each Transmission Operator and each Generator Operator with a Blackstart Resource shall have written Blackstart Resource Agreements or mutually agreed upon procedures or protocols, specifying the terms and conditions of their arrangement. Such Agreements shall include references to the Blackstart Resource testing requirements.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective blackstart resource agreements.
EOP-008-2	R1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a current Operating Plan describing the manner in which it continues to meet its functional obligations with regard to the reliable operations of the BES in the event that its primary control center functionality is lost. This Operating Plan for backup functionality shall include:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with R1 and its sub-requirements with respect to operation of their respective control centers.
EOP-008-2	R1.1	The location and method of implementation for providing backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.2	A summary description of the elements required to support the backup functionality. These elements shall include:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.2.1.	Tools and applications to ensure that System Operators have situational awareness of the BES.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.2.2.	Data exchange capabilities.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.2.3.	Interpersonal Communications.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.2.4.	Power source(s).	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.2.5.	Physical and cyber security.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.3.	An Operating Process for keeping the backup functionality consistent with the primary control center.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.4.	Operating Procedures, including decision authority, for use in determining when to implement the Operating Plan for backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-008-2	R1.5.	A transition period between the loss of primary control center functionality and the time to fully implement the backup functionality that is less than or equal to two hours.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.6.	An Operating Process describing the actions to be taken during the transition period between the loss of primary control center functionality and the time to fully implement backup functionality elements identified in Requirement R1, Part 1.2. The Operating Process shall include:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.6.1.	A list of all entities to notify when there is a change in operating locations.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.6.2.	Actions to manage the risk to the BES during the transition from primary to backup functionality as well as during outages of the primary or backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R1.6.3.	Identification of the roles for personnel involved during the initiation and implementation of the Operating Plan for backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R2.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have a copy of its current Operating Plan for backup functionality available at its primary control center and at the location providing backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to operation of their respective control centers.
EOP-008-2	R4.	Each Balancing Authority and Transmission Operator shall have backup functionality (provided either through a facility or contracted services staffed by applicable certified operators when control has been transferred to the backup functionality location) that includes monitoring, control, logging, and alarming sufficient for maintaining compliance with all Reliability Standards that are applicable to a Balancing Authority's and Transmission Operator's primary control center functionality. To avoid requiring tertiary functionality, backup functionality is not required during: • Planned outages of the primary or backup functionality of two weeks or less • Unplanned outages of the primary or backup functionality	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its backup functionality for its primary control center.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-008-2	R5.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator, shall annually review and approve its Operating Plan for backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its Operating Plan for backup functionality.
EOP-008-2	R5.1.	An update and approval of the Operating Plan for backup functionality shall take place within sixty calendar days of any changes to any part of the Operating Plan described in Requirement R1.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its Operating Plan for backup functionality.
EOP-008-2	R6	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have primary and backup functionality that do not depend on each other for the control center functionality required to maintain compliance with Reliability Standards.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to operation of their respective control centers.
EOP-008-2	R7.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct and document results of an annual test of its Operating Plan that demonstrates:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its annual test of its Operating Plan.
EOP-008-2	R7.1.	The transition time between the simulated loss of primary control center functionality and the time to fully implement the backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its annual test of its Operating Plan.
EOP-008-2	R7.2.	The backup functionality for a minimum of two continuous hours.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its annual test of its Operating Plan.
EOP-008-2	R8.	Each Reliability Coordinator, Balancing Authority, and Transmission Operator that has experienced a loss of its primary or backup functionality and that anticipates that the loss of primary or backup functionality will last for more than six calendar months shall provide a plan to its Regional Entity within six calendar months of the date when the functionality is lost, showing how it will re-establish primary or backup functionality.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with respect to its primary or backup functionality.
EOP-010-1	R3	Each Transmission Operator shall develop, maintain, and implement a GMD Operating Procedure or Operating Process to mitigate the effects of GMD events on the reliable operation of its respective system. At a minimum, the Operating Procedure or Operating Process shall include:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
EOP-010-1	R3.1	Steps or tasks to receive space weather information.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-010-1	R3.2	System Operator actions to be initiated based on predetermined conditions.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
EOP-010-1	R3.3	The conditions for terminating the Operating Procedure or Operating Process.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
EOP-011-4	R1.	Each Transmission Operator shall develop, maintain, and implement one or more Reliability Coordinator-reviewed Operating Plan(s) to mitigate operating Emergencies in its Transmission Operator Area. The Operating Plan(s) shall include the following, as applicable:	X	X	Each	The CAISO and TE will each have an Operating Plan as set forth in R1. The CAISO and the TE's operating plans shall include, to the extent applicable, the R1 sub-requirements as detailed below.
EOP-011-4	1.1.	Roles and responsibilities for activating the Operating Plan(s);	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Operating Plans.
EOP-011-4	1.2.	Processes to prepare for and mitigate Emergencies including:	X	X	Each	The CAISO and the TE shall each separately include processes to prepare for and mitigate Emergencies in their respective Operating Plans to the extent applicable in the R1.2 sub-requirements detailed below.
EOP-011-4	1.2.1.	Notification to its Reliability Coordinator, to include current and projected conditions, when experiencing an operating Emergency;	X		Single	
EOP-011-4	1.2.2.	Cancellation or recall of Transmission and generation outages;	X	X	Split	The ISO and TE shall each have processes for the cancellation or recall of Transmission outages. The ISO shall have a process for the cancellation or recall of generation outages.
EOP-011-4	1.2.3.	Transmission system reconfiguration;	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Operating Plans.
EOP-011-4	1.2.4.	Redispatch of generation request;	X		Single	
EOP-011-4	1.2.5.	Operator-controlled manual Load shed, undervoltage load shed (UVLS), or underfrequency load shed (UFLS) during an Emergency that accounts for each of the following:		X	Single	Effective date: 4/1/2027
EOP-011-4	1.2.5.1.	Provisions for manual Load shedding capable of being implemented in a timeframe adequate for mitigating the Emergency;		X	Single	Effective date: 4/1/2027
EOP-011-4	1.2.5.2.	Provisions to minimize the overlap of circuits that are designated for manual Load shed, UVLS, or UFLS and circuits that serve designated critical loads which are essential to the reliability of the BES;		X	Single	Effective date: 4/1/2027

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
EOP-011-4	1.2.5.3.	Provisions to minimize the overlap of circuits that are designated for manual Load shed and circuits that are utilized for UFLS or UVLS;		X	Single	Effective date: 4/1/2027
EOP-011-4	1.2.5.4.	Provisions for limiting the utilization of UFLS or UVLS circuits for manual Load shed to situations where warranted by system conditions;		X	Single	Effective date: 4/1/2027
EOP-011-4	1.2.5.5.	Provisions for the identification and prioritization of designated critical natural gas infrastructure loads which are essential to the reliability of the BES as defined by the Applicable Entity; and		X	Single	Effective date: 4/1/2027
EOP-011-4	1.2.6.	Provisions to determine reliability impacts of:	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Operating Plans.
EOP-011-4	1.2.6.1.	Cold weather conditions; and	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Operating Plans.
EOP-011-4	1.2.6.2.	Extreme weather conditions.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Operating Plans.
EOP-011-4	R4.	Each Transmission Operator and Balancing Authority shall address any reliability risks identified by its Reliability Coordinator pursuant to Requirement R3 and resubmit its Operating Plan(s) to its Reliability Coordinator within a time period specified by its Reliability Coordinator.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective Operating Plans.
EOP-011-4	R7.	Each Transmission Operator shall annually identify and notify Distribution Providers, UFLS-Only Distribution Providers and Transmission Owners that are required to assist with the mitigation of operating Emergencies in its Transmission Operator Area through operator-controlled manual Load shedding, undervoltage Load shedding, or underfrequency Load shedding		X	Single	
FAC-014-3	R2.	Each Transmission Operator shall establish System Operating Limits (SOLs) for its portion of the Reliability Coordinator Area in accordance with its Reliability Coordinator's SOL methodology.	X		Single	
FAC-014-3	R3.	Each Transmission Operator shall provide its SOLs to its Reliability Coordinator.	X		Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
IRO-001-4	R2.	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall comply with its Reliability Coordinator's Operating Instructions unless compliance with the Operating Instructions cannot be physically implemented or unless such actions would violate safety, equipment, regulatory, or statutory requirements.	X	X	Each	The CAISO and TE shall each separately maintain compliance with this requirement with respect to their respective operations.
IRO-001-4	R3.	Each Transmission Operator, Balancing Authority, Generator Operator, and Distribution Provider shall inform its Reliability Coordinator of its inability to perform the Operating Instruction issued by its Reliability Coordinator in Requirement R1.	X	X	Each	The CAISO and TE shall each separately maintain compliance with this requirement with respect to their respective operations.
IRO-010-5	R3.	Each Reliability Coordinator, Balancing Authority, Generator Owner, Generator Operator, Transmission Operator, Transmission Owner, and Distribution Provider receiving a specification(s) in Requirement R2 shall satisfy the obligations of the documented specifications.	X	X	Each	The CAISO and TE shall each maintain compliance with this requirement with respect to its operations as identified in agreed upon procedure(s) established by the CAISO.
IRO-017-1	R2.	Each Transmission Operator and Balancing Authority shall perform the functions specified in its Reliability Coordinator's outage coordination process.	X		Single	
MOD-033-3	R2.	Each Reliability Coordinator and Transmission Operator shall, within 30 calendar days of a written request, provide actual System behavior data (or a written response that it does not have the requested data) to any Planning Coordinator performing Model Validation under Requirement R1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
NUC-001-4	R2.	The Nuclear Plant Generator Operator and the applicable Transmission Entities shall have in effect one or more Agreements that include mutually agreed to NPIRs and document how the Nuclear Plant Generator Operator and the applicable Transmission Entities shall address and implement these NPIRs	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operations
NUC-001-4	R3.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall incorporate the NPIRs into their planning analyses of the electric system and shall communicate the results of these analyses to the Nuclear Plant Generator Operator.			N/A	This requirement is not applicable to the TOP function. Based upon the NUC agreement, this requirement is applicable to Transmission Planning and Planning Coordinator/Authority.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
NUC-001-4	R4.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement as applicable pursuant to the terms of the Nuclear Agreement.
NUC-001-4	R4.1	Incorporate the NPIRs into their operating analyses of the electric system.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement as applicable pursuant to the terms of the Nuclear Agreement.
NUC-001-4	R4.2	Operate the electric system to meet the NPIRs.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement as applicable pursuant to the terms of the Nuclear Agreement.
NUC-001-4	R4.3	Inform the Nuclear Plant Generator Operator when the ability to assess the operation of the electric system affecting NPIRs is lost.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement as applicable pursuant to the terms of the Nuclear Agreement.
NUC-001-4	R6.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities and the Nuclear Plant Generator Operator shall coordinate outages and maintenance activities which affect the NPIRs.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement as applicable pursuant to the terms of the Nuclear Agreement.
NUC-001-4	R8.	Per the Agreements developed in accordance with this standard, the applicable Transmission Entities shall inform the Nuclear Plant Generator Operator of actual or proposed changes to electric system design (e.g., protective relay setpoints), configuration, operations, limits, or capabilities that may impact the ability of the electric system to meet the NPIRs.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with this requirement as applicable pursuant to the terms of the Nuclear Agreement.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
NUC-001-4	R9.	R9. The Nuclear Plant Generator Operator and the applicable Transmission Entities shall include the following elements in aggregate within the Agreement(s) identified in R2. • Where multiple Agreements with a single Transmission Entity are put into effect, the R9 elements must be addressed in aggregate within the Agreements; however, each Agreement does not have to contain each element. The Nuclear Plant Generator Operator and the Transmission Entity are responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements. • Where Agreements with multiple Transmission Entities are required, the Nuclear Plant Generator Operator is responsible for ensuring all the R9 elements are addressed in aggregate within the Agreements with the Transmission Entities. The Agreements with each Transmission Entity do not have to contain each element; however, the Agreements with the multiple Transmission Entities, in the aggregate, must address all R9 elements. For each Agreement(s), the Nuclear Plant Generator Operator and the Transmission Entity are responsible to ensure the Agreement(s) contain(s) the elements of R9 applicable to that Transmission Entity.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.2	Technical requirements and analysis:	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.2.1.	Identification of parameters, limits, configurations, and operating scenarios included in the NPIRs and, as applicable, procedures for providing any specific data not provided within the Agreement.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.2.2.	Identification of facilities, components, and configuration restrictions that are essential for meeting the NPIRs.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.2.3.	Types of planning and operational analyses performed specifically to support the NPIRs, including the frequency of studies and types of Contingencies and scenarios required.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.	Operations and maintenance coordination	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
NUC-001-4	R9.3.1.	Designation of ownership of electrical facilities at the interface between the electric system and the nuclear plant and responsibilities for operational control coordination and maintenance of these facilities.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.2.	Identification of any maintenance requirements for equipment not owned or controlled by the Nuclear Plant Generator Operator that are necessary to meet the NPIRs.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.3.	Coordination of testing, calibration and maintenance of on-site and off-site power supply systems and related components.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.4.	Provisions to address mitigating actions needed to avoid violating NPIRs and to address periods when responsible Transmission Entity loses the ability to assess the capability of the electric system to meet the NPIRs. These provisions shall include responsibility to notify the Nuclear Plant Generator Operator within a specified time frame.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.5.	Provision for considering, within the restoration process, the requirements and urgency of a nuclear plant that has lost all off-site and on-site AC power.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.6.	Coordination of physical and cyber security protection at the nuclear plant interface to ensure each asset is covered under at least one entity's plan.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.3.7.	Coordination of the NPIRs with transmission system Remedial Action Schemes and any programs that reduce or shed load based on underfrequency or undervoltage.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.4.	Communications and training Administrative elements:	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.4.1.	Provisions for communications affecting the NPIRs between the Nuclear Plant Generator Operator and Transmission Entities, including communications protocols, notification time requirements, and definitions of applicable unique terms	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
NUC-001-4	R9.4.2.	Provisions for coordination during an off-normal or emergency event affecting the NPIRs, including the need to provide timely information explaining the event, an estimate of when the system will be returned to a normal state, and the actual time the system is returned to normal.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.4.3.	Provisions for coordinating investigations of causes of unplanned events affecting the NPIRs and developing solutions to minimize future risk of such events.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.4.4.	Provisions for supplying information necessary to report to government agencies, as related to NPIRs.	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
NUC-001-4	R9.4.5.	Provisions for personnel training, as related to NPIRs	x	x	Each	The CAISO and the TE shall each be party to a Nuclear Agreement with the Nuclear Plant Generator Operator
PER-003-2	R2.	Each Transmission Operator shall staff its Real-time operating positions performing Transmission Operator reliability-related tasks with System Operators who have demonstrated minimum competency in the areas listed by obtaining and maintaining one of the following valid NERC certificates:	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-003-2	R2.1	Areas of Competency	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-003-2	R2.1.1	Transmission operations	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-003-2	R2.1.2.	Emergency preparedness and operations	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-003-2	R2.1.3.	System operations	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-003-2	R2.1.4.	Protection and control	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-003-2	R2.1.5.	Voltage and reactive	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
PER-003-2	R2.2.	Certificates • Reliability Operator • Balancing, Interchange and Transmission Operator • Transmission Operator	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement a training program for its System Operators	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R1.1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall create a list of Bulk Electric System (BES) company-specific Real-time reliability-related tasks based on a defined and documented methodology.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R1.1.1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall review, and update if necessary, its list of BES company-specific Real-time reliability-related tasks identified in part 1.1 each calendar year.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R1.2	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall design and develop training materials according to its training program, based on the BES company-specific Real-time reliability-related task list created in part 1.1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R1.3	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall deliver training to its System Operators according to its training program.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R1.4	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct an evaluation each calendar year of the training program established in Requirement R1 to identify any needed changes to the training program and shall implement the changes identified.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R3	Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall verify, at least once, the capabilities of its personnel, identified in Requirement R1 or Requirement R2, assigned to perform each of the BES company-specific Real-time reliability-related tasks identified under Requirement R1 part 1.1 or Requirement R2 part 2.1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
PER-005-2	R3.1	Within six months of a modification or addition of a BES company-specific Real-time reliability-related task, each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner shall verify the capabilities of each of its personnel identified in Requirement R1 or Requirement R2 to perform the new or modified BES company-specific Real-time reliability-related tasks identified in Requirement R1 part 1.1 or Requirement R2 part 2.1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R4	Each Reliability Coordinator, Balancing Authority, Transmission Operator, and Transmission Owner that (1) has operational authority or control over Facilities with established Interconnection Reliability Operating Limits (IROLs), or (2) has established protection systems or operating guides to mitigate IROL violations, shall provide its personnel identified in Requirement R1 or Requirement R2 with emergency operations training using simulation technology such as a simulator, virtual technology, or other technology that replicates the operational behavior of the BES.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R4.1	A Reliability Coordinator, Balancing Authority, Transmission Operator, or Transmission Owner that did not previously meet the criteria of Requirement R4, shall comply with Requirement R4 within 12 months of meeting the criteria.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R5	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall use a systematic approach to develop and implement training for its identified Operations Support Personnel on how their job function(s) impact those BES company-specific Real-time reliability-related tasks identified by the entity pursuant to Requirement R1 part 1.1.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel
PER-005-2	R5.1	Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall conduct an evaluation each calendar year of the training established in Requirement R5 to identify and implement changes to the training.	x	x	Each	The CAISO and the TE shall each separately maintain compliance with respect to their respective operating personnel

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
TOP-001-6	R1.	Each Transmission Operator shall act to maintain the reliability of its Transmission Operator Area via its own actions or by issuing Operating Instructions.	X	X	Each	The CAISO and TE shall each separately maintain compliance with this requirement with respect to their respective operations.
TOP-001-6	R5.	Each Transmission Operator, Generator Operator, and Distribution Provider shall comply with each Operating Instruction issued by its Balancing Authority, unless such action cannot be physically implemented or it would violate safety, equipment, regulatory, or statutory requirements.		X	Single	
TOP-001-6	R6.	Each Transmission Operator, Generator Operator, and Distribution Provider shall inform its Balancing Authority of its inability to comply with an Operating Instruction issued by its Balancing Authority.		X	Single	
TOP-001-6	R7.	Each Transmission Operator shall assist other Transmission Operators within its Reliability Coordinator Area, if requested and able, provided that the requesting Transmission Operator has implemented its comparable Emergency procedures, unless such assistance cannot be physically implemented or would violate safety, equipment, regulatory, or statutory requirements.	X	X	Each	The CAISO and TE shall each separately maintain compliance with this requirement with respect to their respective operations.
TOP-001-6	R8.	Each Transmission Operator shall inform its Reliability Coordinator, known impacted Balancing Authorities, and known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency.	X	X	Split	The CAISO is responsible for informing its RC and any known impacted Balancing Authorities and Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency. The TE is responsible for informing any known impacted Transmission Operators of its actual or expected operations that result in, or could result in, an Emergency.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
TOP-001-6	R9.	Each Balancing Authority and Transmission Operator shall notify its Reliability Coordinator and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities.	X	X	Split	The CAISO is responsible for notifying its RC of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities. The TE is responsible for notifying CAISO and known impacted interconnected entities of all planned outages, and unplanned outages of 30 minutes or more, for telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between the affected entities.
TOP-001-6	R10.	Each Transmission Operator shall perform the following for determining System Operating Limit (SOL) exceedances within its Transmission Operator Area:	X		Single	
TOP-001-6	R10.1.	Monitor Facilities within its Transmission Operator Area;	X		Single	
TOP-001-6	R10.2.	Monitor the status of Remedial Action Schemes within its Transmission Operator Area;	X		Single	
TOP-001-6	R10.3.	Monitor non-BES facilities within its Transmission Operator Area identified as necessary by the Transmission Operator;	X		Single	
TOP-001-6	R10.4.	Obtain and utilize status, voltages, and flow data for Facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator;	X		Single	
TOP-001-6	R10.5.	Obtain and utilize the status of Remedial Action Schemes outside its Transmission Operator Area identified as necessary by the Transmission Operator; and	X		Single	
TOP-001-6	R10.6.	Obtain and utilize status, voltages, and flow data for non-BES facilities outside its Transmission Operator Area identified as necessary by the Transmission Operator.	X		Single	
TOP-001-6	R12.	Each Transmission Operator shall not operate outside any identified Interconnection Reliability Operating Limit (IROL) for a continuous duration exceeding its associated IROL Tv.	X		Single	
TOP-001-6	R13.	Each Transmission Operator shall ensure that a Real-time Assessment is performed at least once every 30 minutes.	X		Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
TOP-001-6	R14.	Each Transmission Operator shall initiate its Operating Plan to mitigate a SOL exceedance identified as part of its Real-time monitoring or Real-time Assessment.	X		Single	
TOP-001-6	R15.	Each Transmission Operator shall inform its Reliability Coordinator of actions taken to return the System to within limits when a SOL has been exceeded in accordance with its Reliability Coordinator's SOL methodology.	X		Single	
TOP-001-6	R16.	Each Transmission Operator shall provide its System Operators with the authority to approve planned outages and maintenance of its telemetering and control equipment, monitoring and assessment capabilities, and associated communication channels between affected entities.	X	X	Each	The CAISO and TE shall each maintain compliance with this requirement with respect to its operations as identified in agreed upon procedure(s) established by the CAISO.
TOP-001-6	R18.	Each Transmission Operator shall operate to the most limiting parameter in instances where there is a difference in SOLs.	X		Single	
TOP-001-6	R20.	Each Transmission Operator shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within the Transmission Operator's primary Control Center, for the exchange of Real-time data with its Reliability Coordinator, Balancing Authority, and the entities it has identified it needs data from in order for it to perform its Real-time monitoring and Real-time Assessments.	X	X	Split	The CAISO shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within its primary Control Center for data exchange of Real-time data with its RC and BA and entities it identifies to allow it to perform Real-time monitoring and Real-Time Assessments. The TE shall have data exchange capabilities, with redundant and diversely routed data exchange infrastructure within its primary Control Center for data exchange of Real-time data with its RC and BA and entities it identifies to allow it to perform Real-time monitoring.
TOP-001-6	R21.	Each Transmission Operator shall test its primary Control Center data exchange capabilities specified in Requirement R20 for redundant functionality at least once every 90 calendar days. If the test is unsuccessful, the Transmission Operator shall initiate action within two hours to restore redundant functionality.	X	X	Each	The CAISO and TE shall each separately maintain compliance with this requirement with respect to their respective primary Control Centers and responsibilities identified in R20.
TOP-001-6	R25.	Each Transmission Operator shall use the applicable Reliability Coordinator's SOL methodology when determining SOL exceedances for Real-time Assessments, Real- time monitoring, and Operational Planning Analysis.	X		Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
TOP-002-5	R1.	Each Transmission Operator shall have an Operational Planning Analysis that will allow it to assess whether its planned operations for the next day within its Transmission Operator Area will exceed any of its System Operating Limits (SOLs).	X		Single	
TOP-002-5	R2.	Each Transmission Operator shall have an Operating Plan(s) for next-day operations to address potential System Operating Limit (SOL) exceedances identified as a result of its Operational Planning Analysis as required in Requirement R1.	X		Single	
TOP-002-5	R3.	Each Transmission Operator shall notify entities identified in the Operating Plan(s) cited in Requirement R2 as to their role in those plan(s).	X		Single	
TOP-002-5	R6.	Each Transmission Operator shall provide its Operating Plan(s) for next day operations identified in Requirement R2 to its Reliability Coordinator.	X		Single	
TOP-003-6.1	R1.	Each Transmission Operator shall maintain documented specification(s) for the data and information necessary for it to perform its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments. The specification shall include, but not be limited to:	X		Single	
TOP-003-6.1	R1.1.	A list of data and information needed by the Transmission Operator to support its Operational Planning Analyses, Real-time monitoring, and Real-time Assessments including non-BES data and information, external network data and information, and identification of the entities responsible for responding to the specification as deemed necessary by the Transmission Operator.	X		Single	
TOP-003-6.1	R1.2.	Provisions for notification of current Protection System and Remedial Action Scheme (RAS) status or degradation that impacts System reliability.	X		Single	
TOP-003-6.1	R1.3.	Provisions for notification of BES generating unit(s) during local forecasted cold weather to include:	X		Single	
TOP-003-6.1	R1.3.1.	Operating limitations based on:	X		Single	
TOP-003-6.1	R1.3.1.1.	capability and availability;	X		Single	
TOP-003-6.1	R1.3.1.2.	fuel supply and inventory concerns;	X		Single	
TOP-003-6.1	R1.3.1.3.	fuel switching capabilities; and	X		Single	
TOP-003-6.1	R1.3.1.4.	environmental constraints	X		Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
TOP-003-6.1	R1.4.	Identification of a mutually agreeable process for resolving conflicts.	X		Single	
TOP-003-6.1	R1.5.	Method(s) for the entity identified in Part 1.1 to provide the data and information that includes at a minimum the following.	X		Single	
TOP-003-6.1	R1.5.2.	Performance criteria for the availability and accuracy of data and information as applicable;	X		Single	
TOP-003-6.1	R1.5.3.	Provisions to update or correct data and information, as applicable or necessary;	X		Single	
TOP-003-6.1	R1.5.4.	A mutually agreeable format;	X		Single	
TOP-003-6.1	R1.5.5.	Mutually agreeable method(s) for securely transferring data and information.	X		Single	
TOP-003-6.1	R1.5.1.	Specified deadlines or periodicity which data and information is to be provided;	X		Single	
TOP-003-6.1	R3.	Each Transmission Operator shall distribute its data and information specification(s) to entities that have data and information required by the Transmission Operator's Operational Planning Analyses, Real- time monitoring, and Real-time Assessments.	X		Single	
TOP-003-6.1	R5.	Each Transmission Operator, Balancing Authority, Generator Owner, Generator Operator, Transmission Owner, and Distribution Provider receiving a data and information specification(s) in Requirement R3 or R4 shall satisfy the obligations of the documented specifications.	X	X	Each	The CAISO and TE shall each maintain compliance with this requirement with respect to its operations as identified in agreed upon procedure(s) established by the CAISO.
TOP-010-1(i)	R1.	Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The Operating Process or Operating Procedure shall include:	X	X	Split	The CAISO shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring and Real-time Assessments. The TE shall implement an Operating Process or Operating Procedure to address the quality of the Real-time data necessary to perform its Real-time monitoring.
TOP-010-1(i)	R1.1.	Criteria for evaluating the quality of Real-time data;	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
TOP-010-1(i)	R1.2.	Provisions to indicate the quality of Real-time data to the System Operator; and	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
TOP-010-1(i)	R1.3.	Actions to address Real-time data quality issues with the entity(ies) responsible for providing the data when data quality affects Real-time Assessments.	X		Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
TOP-010-1(i)	R3.	Each Transmission Operator shall implement an Operating Process or Operating Procedure to address the quality of analysis used in its Real-time Assessments. The Operating Process or Operating Procedure shall include:	X		Single	
TOP-010-1(i)	R3.1.	Criteria for evaluating the quality of analysis used in its Real-time Assessments;	X		Single	
TOP-010-1(i)	R3.2.	Provisions to indicate the quality of analysis used in its Real-time Assessments; and	X		Single	
TOP-010-1(i)	R3.3.	Actions to address analysis quality issues affecting its Real-time Assessments.	X		Single	
TOP-010-1(i)	R4.	Each Transmission Operator and Balancing Authority shall have an alarm process monitor that provides notification(s) to its System Operators when a failure of its Real-time monitoring alarm processor has occurred.	X	X	Each	The CAISO and the TE shall each separately maintain compliance with this requirement with respect to their respective operations.
VAR-001-5	R1.	Each Transmission Operator shall specify a system voltage schedule (which is either a range or a target value with an associated tolerance band) as part of its plan to operate within System Operating Limits and Interconnection Reliability Operating Limits.		x	Single	
VAR-001-5	R1.1.	Each Transmission Operator shall provide a copy of the voltage schedules (which is either a range or a target value with an associated tolerance band) to its Reliability Coordinator and adjacent Transmission Operators within 30 calendar days of a request.		x	Single	
VAR-001-5	R2.	Each Transmission Operator shall schedule sufficient reactive resources to regulate voltage levels under normal and Contingency conditions. Transmission Operators can provide sufficient reactive resources through various means including, but not limited to, reactive generation scheduling, transmission line and reactive resource switching, and using controllable load.	x	x	Split	The ISO is responsible for this requirement with respect to the scheduling of reactive resource facilities it has operational control over, including but not limited to generation and transmission lines. The TE is responsible for this requirement with respect to the scheduling of reactive resource facilities it has operational control over, including but not limited to transmission lines, reactive resource switching and the use of controllable load.
VAR-001-5	R3.	Each Transmission Operator shall operate or direct the Real-time operation of devices to regulate transmission voltage and reactive flow as necessary.	x	x	Each	The CAISO and TE shall each separately maintain compliance with this requirement with respect to their respective operations.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
VAR-001-5	R4.	The Transmission Operator shall specify the criteria that will exempt generators: 1) from following a voltage or Reactive Power schedule, 2) from having its automatic voltage regulator (AVR) in service or from being in voltage control mode, or 3) from having to make any associated notifications.			N/A	This requirement has been superseded by a WECC regional variance.
VAR-001-5	R4.1.	If a Transmission Operator determines that a generator has satisfied the exemption criteria, it shall notify the associated Generator Operator.			N/A	This requirement has been superseded by a WECC regional variance.
VAR-001-5	R5.	Each Transmission Operator shall specify a voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) at either the high voltage side or low voltage side of the generator step-up transformer at the Transmission Operator's discretion.			N/A	This requirement has been superseded by a WECC regional variance.
VAR-001-5	R5.1.	The Transmission Operator shall provide the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (the AVR is in service and controlling voltage).			N/A	This requirement has been superseded by a WECC regional variance.
VAR-001-5	R5.2.	The Transmission Operator shall provide the Generator Operator with the notification requirements for deviations from the voltage or Reactive Power schedule (which is either a range or a target value with an associated tolerance band).			N/A	This requirement has been superseded by a WECC regional variance.
VAR-001-5	R5.3.	The Transmission Operator shall provide the criteria used to develop voltage schedules Reactive Power schedule (which is either a range or a target value with an associated tolerance band) to the Generator Operator within 30 days of receiving a request.			N/A	This requirement has been superseded by a WECC regional variance.

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

			Responsibility			
Standard	**Req.**	**Text of Requirement**	**CAISO**	**TE**	**Responsibility (either Each, Split, Single or N/A)**	**Responsibility Details**
VAR-001-5	E.A.13	Each Transmission Operator shall issue any one of the following types of voltage schedules to the Generator Operators for each of their generation resources that are on-line and part of the Bulk Electric System within the Transmission Operator Area: • A voltage set point with a voltage tolerance band and a specified period. • An initial volt-ampere reactive output or initial power factor output with a voltage tolerance band for a specified period that the Generator Operator uses to establish a generator bus voltage set point. • A voltage band for a specified period.		x	Single	
VAR-001-5	E.A.14	Each Transmission Operator shall provide one of the following voltage schedule reference points for each generation resource in its area to the Generator Operator. • The generator terminals. • The high side of the generator step-up transformer. • The point of interconnection. • A location designated by mutual agreement between the Transmission Operator and Generator Operator.		x	Single	
VAR-001-5	E.A.16	Each Transmission Operator shall provide to the Generator Operator, within 30 calendar days of a request for data by the Generator Operator, its transmission equipment data and operating data that supports development of the voltage set point conversion methodology.		x	Single	
VAR-001-5	R6.	After consultation with the Generator Owner regarding necessary step-up transformer tap changes and the implementation schedule, the Transmission Operator shall provide documentation to the Generator Owner specifying the required tap changes, a timeframe for making the changes, and technical justification for these changes.		x	Single	

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

Matrix Revision History

Version	Standard	Change	Date
1.0	All	Original CFR matrix developed	12/9/2014
2.0	EOP-010-1	New Standard	2/18/2015
2.0	VAR-002-WECC-2	Substituted VAR-002-WECC-2 for VAR-002-WECC-1	3/27/2015
3.0	CIP-014-1	New Standard (Effective 10/1/2015-10/2/2015)	9/24/2015
3.0	CIP-014-2	New Standard (Effective 10/2/2015)	9/24/2015
3.0	COM-001-2	Substituted COM-001-2 for COM-001-1.1	9/24/2015
4.0	NUC-001-3	Substituted NUC-001-3 for NUC-001-2	12/8/2015
5.0	COM-002-4	Substituted COM-002-4 for COM-002-2	6/14/2016
5.0	PER-005-2	Substituted PER-005-2 for PER-005-1	6/14/2016
5.0	CIP-002-5.1	Substituted CIP-002-5.1 for CIP-002-3	6/14/2016
5.0	CIP-003-6	Substituted CIP-003-6 for CIP-003-3	6/14/2016
5.0	CIP-004-6	Substituted CIP-004-6 for CIP-004-3	6/14/2016
5.0	CIP-005-5	Substituted CIP-005-5 for CIP-005-3	6/14/2016
5.0	CIP-006-6	Substituted CIP-006-6 for CIP-006-3	6/14/2016
5.0	CIP-007-6	Substituted CIP-007-6 for CIP-007-3	6/14/2016
5.0	CIP-008-5	Substituted CIP-008-5 for CIP-008-3	6/14/2016
5.0	CIP-009-6	Substituted CIP-009-6 for CIP-009-3	6/14/2016
5.0	CIP-010-2	New Standard	6/14/2016
5.0	CIP-011-2	New Standard	6/14/2016
5.0	CIP-014-1	Remove CIP-014-1	6/14/2016
5.0	MOD-028-2	Remove MOD-028-2 R3.2.2 and R3.2.3	6/14/2016
6.0	TOP-003-3	New Standard (R1 and R3 Only)	10/25/2016
7.0	EOP-001-2.1b	Retired (Replaced with EOP-011-1)	3/21/2017
7.0	EOP-003-2	Retired (Replaced with EOP-011-1)	3/21/2017
7.0	EOP-004-3	Substituted EOP-004-3 for EOP-004-2	3/21/2017
7.0	EOP-011-1	New Standard	3/21/2017
7.0	IRO-001-4	Substituted IRO-001-4 for IRO-001-1.1	3/21/2017
7.0	IRO-004-2	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	IRO-005-3a	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	IRO-010-2	Substituted IRO-010-2 for IRO-010-1a	3/21/2017
7.0	IRO-017-1	New Standard	3/21/2017
7.0	MOD-029-2a	Substituted MOD-029-2a for MOD-029-1a	3/21/2017

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

Version	Standard	Change	Date
7.0	MOD-030-3	Substituted MOD-030-3 for MOD-030-2	3/21/2017
7.0	PER-001-0.2	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	PRC-004-WECC-2	Substituted PRC-004-WECC-2 for PRC-004-WECC-1	3/21/2017
7.0	TOP-001-3	Substituted TOP-001-3 for TOP-001-1a	3/21/2017
7.0	TOP-002-4	Substituted TOP-002-4 for TOP-002-2.1b	3/21/2017
7.0	TOP-003-3	Substituted TOP-003-3 for TOP-003-1	3/21/2017
7.0	TOP-004-2	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	TOP-005-2a	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	TOP-006-2	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	TOP-007-0	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
7.0	TOP-008-1	Retired (Replaced with TOP/IRO revised standards)	3/21/2017
8.0	PRC-010-0	Remove PRC-010-0 - no longer applicable to the TOP function	6/21/2017
8.0	PRC-022-1	Remove PRC-022-1 - retired 3/31/2017	6/21/2017
8.0	TOP-007-WECC-1	Remove TOP-007-WECC-1 - retired 3/10/2017	6/21/2017
8.0	MOD-033-1	New Standard	6/21/2017
9.0	COM-001-3	Substituted COM-001-3 for COM-001-2	9/20/2017
10.0	CIP-002-5.1a	Substituted CIP-002-5.1a for CIP-002-5.1	3/14/2018
10.0	PRC-001-1.1(ii)	Substituted PRC-001-1.1(ii) for PRC-001-1	3/14/2018
10.0	VAR-001-4.2	Substituted VAR-001-4.2 for VAR-001-4	3/14/2018
10.0	TOP-010-1(i)	New Standard	2/9/2018
11.0	TOP-001-4	Substituted TOP-001-4 for TOP-001-3	5/16/2018
12.0	BAL-005-0.2b	Removed BAL-005-0.2b; no longer applicable to TOP function	12/23/2018
12.0	VAR-001-5	Substituted VAR-001-5 for VAR-001-4.2	12/23/2018
12.0	VAR-002-WECC-2	Remove VAR-002-WECC-2 - retired 9/5/2018	12/23/2018
13.0	EOP-004-4	Substituted EOP-004-4 for EOP-004-3	3/12/2019
13.0	EOP-005-3	Substituted EOP-005-3 for EOP-005-2	3/12/2019
13.0	EOP-008-2	Substituted EOP-008-2 for EOP-008-1	3/12/2019
13.0	PRC-001-1.1(ii)	Removed R2, R5, R6 - Retired 3/31/2017	3/12/2019
14.0	N/A	Minor fixes to TOP-002-4 R6 blank column; PRC-004-WECC-2 R2.3.2 fix requirement number	6/19/2019
14.0	PER-003-2	Substituted PER-003-2 for PER-003-1	6/19/2019
15.0	CIP-003-7	Substituted CIP-003-7 for CIP-003-6	12/11/2019
16.0	CIP-003-8	Substituted CIP-003-8 for CIP-003-7	3/16/2020
17.0	CIP-005-6	Substituted CIP-005-6 for CIP-005-5	9/17/2020

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

Version	Standard	Change	Date
17.0	CIP-010-3	Substituted CIP-010-3 for CIP-010-2	9/17/2020
17.0	CIP-013-1	New Standard	9/17/2020
18.0	CIP-008-6	Substituted CIP-008-6 for CIP-008-5	12/4/2020
18.0	PRC-004-WECC-2	Removed PRC-004-WECC-2 - retired 1/1/2021	12/4/2020
19.0	IRO-010-3	Substituted IRO-010-3 for IRO-010-2	3/15/2021
19.0	MOD-033-2	Substituted MOD-033-2 for MOD-033-1	3/15/2021
19.0	NUC-001-4	Substituted NUC-001-4 for NUC-001-3	3/15/2021
19.0	TOP-001-5	Substituted TOP-001-5 for TOP-001-4	3/15/2021
19.0	TOP-003-4	Substituted TOP-003-4 for TOP-003-3	3/15/2021
20.0	PRC-001-1(ii)	Remove PRC-001-1(ii) - Retired 3/31/2021	6/2/2022
20.0	CIP-012-1	New Standard	6/2/2022
21.0	CIP-005-7	Substituted CIP-005-7 for CIP-005-6	9/20/2022
21.0	CIP-010-4	Substituted CIP-010-4 for CIP-010-3	9/20/2022
21.0	CIP-013-2	Substituted CIP-013-2 for CIP-013-1	9/20/2022
22.0	EOP-011-2	Substituted EOP-011-2 for EOP-011-1	3/17/2023
22.0	IRO-010-4	Substituted IRO-010-4 for IRO-010-3	3/17/2023
22.0	TOP-003-5	Substituted TOP-003-5 for TOP-003-4	3/17/2023
23.0	CIP-004-7	Substituted CIP-004-7 for CIP-004-6	12/28/2023
23.0	CIP-011-3	Substituted CIP-011-3 for CIP-011-2	12/28/2023
24.0	FAC-014-3	Substituted FAC-014-3 for FAC-014-2	3/6/2024
24.0	TOP-001-6	Substituted TOP-001-6 for TOP-001-5	3/6/2024
24.0	CIP-014-3	Substituted CIP-014-3 for CIP-014-2	3/6/2024
24.0	MOD-001-1a	Removed MOD-001-1a - retired 2/1/2024	3/6/2024
24.0	MOD-008-1	Removed MOD-008-1 - retired 2/1/2024	3/6/2024
24.0	MOD-028-2	Removed MOD-028-2 - retired 2/1/2024	3/6/2024
24.0	MOD-029-2a	Removed MOD-029-2a- retired 2/1/2024	3/6/2024
24.0	MOD-030-3	Removed MOD-030-3 - retired 2/1/2024	3/6/2024
25.0	EOP-011-4	Substituted EOP-011-4 for EOP-011-2; effective date of R1.2.5 and its sub-requirements is 4/1/2027	9/9/2024
26.0	IRO-010-5	Substituted IRO-010-5 for IRO-001-4	6/17/2025
26.0	TOP-003-6.1	Substituted TOP-003-6.1 for TOP-003-5	6/17/2025
27.0	TOP-002-5	Substituted TOP-002-5 for TOP-002-4	8/26/2025
28.0	CIP-003-9 & MOD-033-3	Substituted CIP-003-8 for CIP-003-9 and MOD-033-2 for MOD-033-3	3/18/2026

APPENDIX 3: CFR Matrix for Coordinated Functional Registration Agreement Between California ISO and Pacific Gas and Electric
Version 28.0

Version	Standard	Change	Date

Signed by:
John Phipps
3C5F64BF6B65411...

4/15/2026

CAISO Authorized Representative — Date

Signed by:
Roderick Robinson
A66B1A2D55A4B0...

4/9/2026

TE Authorized Representative — Date