No.	New Rule	Page No.	PD Section Header and No.
1	***Each Operator will develop and implement a Mitigation Plan.***	2	Summary
2	The Mitigation Plans will follow a six-step procedure for carrying out these new physical security plan requirements, modeled on security plan requirements set forth by the North America Electric Reliability Corporation (NERC) CIP-014.	2, 33	Summary
3	Within 24 months of this decision, the IOUs will be required to submit their Final Security Plan Report. ***Within 30 months, each of the Publicly Owned Utilities (POUs) will be required to provide the Commission with notice that a validated plan has been adopted.***	2, 33	Summary, 6.6 Timeline for Implementation
4	Costs of incremental physical security measures should be reasonable, controlled, and weighed against potential benefit, so they do not result in a burden to ratepayers.	32	6. Guiding Principles of California Electric Physical Security
5	Opportunities to incorporate high-benefit, low-cost measures should be captured, particularly at the time of new or upgraded substation construction.	32	6. Guiding Principles of California Electric Physical Security
6	Distribution assets to be hardened or designated with consideration for ensuring service integrity to essential customers, among other factors identified in the Joint Proposal.	32	6. Guiding Principles of California Electric Physical Security

No.	New Rule	Page No.	PD Section Header and No.
7	**Resiliency strategies to ensure that priority distribution assets, particularly those tied to service of essential customers remain in service and are able to rapidly recover from an unplanned service outage should be considered an equally effective response to addressing physical security risks.**	**32**	**6. Guiding Principles of California Electric Physical Security**
8	**Step 1. Assessment. Drafting of a plan, addressing prevention, response, and recovery, which could be prepared in-house or by a consultant, and which shall include proposed and recommended mitigation measures.**	**33**	**6.1 Six-Step Procedure to Address Utilities' Distribution Assets**
9	**Step 2. Independent Review and Utility Response to Recommendations. Proposed plan would be "reviewed" and deemed appropriate and adequate by an independent third party, likely a qualified consultant expert, national laboratory, or a regulatory or industry standard body (such as the Electric Power Research Institute). Step 2 would include reviewer recommendations that assess and appraise the appropriateness of the risk assessment, proposed mitigation measures, and other plan elements. A utility would be expected to fully address reviewer recommendations, including justifying any mitigations that it declines to accept; the independent third-party opinion/recommendations, utility response, threat and risk assessment, and mitigation measures combined would constitute a final plan report.**	**33**	**6.1 Six-Step Procedure to Address Utilities' Distribution Assets**

No.	New Rule	Page No.	PD Section Header and No.
10	**Step 3. Validation (for IOUs only). Final plan report would be validated (recurring every five years) so as to deem it adequate, in compliance, and eligible to request funding for implementation. The validation would be performed by the CPUC SED. Non-compliance would be met with a violation order, potentially resulting in sanctions and/or penalties as provided by PU Code Sec. 364(c). Step 3 completion would render eligible for funding appropriate physical security needs identified by IOUs; such project funding would be linked, tracked, and authorized according to approved CPUC mechanisms.**	**33**	**6.1 Six-Step Procedure to Address Utilities' Distribution Assets**
11	**Step 3a. Validation (for POUs only). Final plan report would be validated (recurring every five years, and eligible for same exemption request process made available to the IOUs) by a qualified authority designated by the applicable local governance body. (For example, Riverside Public Utilities currently develops a security and emergency response plan that conforms to the Governor's Office of Emergency Services (CalOES) and Federal Emergency Management Agency (FEMA) standards and receives their endorsement.)**	**34**	**6.1 Six-Step Procedure to Address Utilities' Distribution Assets**
12	**Step 4. Adoption (for POUs only). Validated plan would be submitted to the appropriate regulatory oversight body (local governance body) for review and greenlighting (adoption). Step 4 should include funding to implement the plan.**	**34**	**6.1 Six-Step Procedure to Address Utilities' Distribution Assets**

No.	New Rule	Page No.	PD Section Header and No.
13	Step 4a. Notice. (for POUs only). Provide CPUC with official notice adopted plan action (ideally including a copy of a resolution).	34	6.1 Six-Step Procedure to Address Utilities' Distribution Assets
14	Step 5. Maintenance. Ongoing adopted plan refinement and updates as appropriate and as necessary to preserve plan integrity. All security plans should be concurrent with and integrated into utility resiliency plans and activities.	35	6.1 Six-Step Procedure to Address Utilities' Distribution Assets
15	Step 6. Repeat Process. Plan overhaul and new validation after every five years.	35	6.1 Six-Step Procedure to Address Utilities' Distribution Assets
16	1. California electric utilities, shall within any new or renovated distribution substation, incorporate and design their facilities to incorporate reasonable security features.	35	6.2 Additional Requirements for Mitigation Plans

No.	New Rule	Page No.	PD Section Header and No.
17	**2. Utilities' security plans shall include a detailed narrative explaining how the utility is taking steps to implement: (a) An asset management program to promote optimization and quality assurance for tracking and locating spare parts stock, ensuring availability and the rapid dispatch of available spare parts; (b) A robust workforce training and retention program to employ a full roster of highly-qualified service technicians able to respond to make repairs in short order throughout a utility's service territory using spare parts stockpiles and inventory; (c) A preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately; and, (d) A description of Distribution Control Center and Security Control Center roles and actions related to distribution system physical security (this item would be for IOUs only).**	**35**	**6.2 Additional Requirements for Mitigation Plans**
18	**The third-party reviewer shall prepare recommendations on appropriate mitigation measures and/or a statement supporting or rejecting proposed mitigation measures. This statement shall contain justification for the acceptance or rejection of each proposed mitigation measures.**	**36**	**6.3 Third-Party Verification**
19	**Each utility shall produce a response to these proposed mitigation measures and the third-party expert's opinion and recommendations, indicating whether it concurs or disagrees, and whether a given mitigation measure will be implemented, or is declined. Utilities should provide a justification for declining any proposed mitigation measures**	**37**	**6.3 Third-Party Verification**

No.	New Rule	Page No.	PD Section Header and No.
20	A utility's risk-threat assessment, mitigation plan, consultant appraisal and statement, and utility response, would together comprise its Security Plan Report.	37	6.3 Third-Party Verification
21	The Security Plan Report should include an estimated timeframe for how long it will take to complete and a cost estimate for incremental expenses associated with implementing the plan.	37	6.3 Third-Party Verification
22	The Unaffiliated Third-Party Reviewer shall be an entity other than the Operator with appropriate expertise, as described below. The selected third-party reviewer cannot be a corporate affiliate of the Operator (i.e., the third-party reviewer cannot be an entity that its controlled by the utility, is controlled by or is under common control with, the Operator). A third-party reviewer also cannot be a division of the Operator that operates as a functional unit. A governmental entity can select as the third-party reviewer another governmental entity within the same political subdivision, so long as the entity has the appropriate expertise, and is not a division of the Operator that operates as a functional unit, i.e., a municipality could use its police department as its third-party reviewer if it has the appropriate expertise.	37	6.4 Third-Party Expert Qualifications

No.	New Rule	Page No.	PD Section Header and No.
23	**The Unaffiliated Third-Party Reviewer shall be an entity or organization with: electric industry physical security experience and whose review staff has appropriate physical security expertise, i.e., have at least one member who holds either an ASIS International Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; an entity or organization with demonstrated law enforcement, government, or military physical security expertise; or an entity or organization approved to do physical security assessments by the CPUC, Electric Reliability Organization or similar electrical industry regulatory body.**	32	6.4 Third-Party Expert Qualifications
24	**This approach shall be superseded when the Commission finalizes its rules for the safekeeping, sharing, transmittal, and inspection of confidential information. In the event that theis approach is still in effect 24 months after the date of adoption of this decision, review and revision of the approach may be requested by a petition to modify.**	38	6.5 Access to Information
25	**The Reading Room approach shall entail utility information being made available to Commission staff on utility property at a location convenient and agreed to by CPUC staff.**	38	6.5 Access to Information
26	**It remains without question that the Commission and its staff require and are fully entitled to access to such information, as long as protections against public release are maintained. Especially in cases where the Commission is investigating an incident (whether it is already defined in our regulations or a new aspect, such as physical or cyber-attack), access to records shall be provided upon the Commission request.**	38	6.5 Access to Information

No.	New Rule	Page No.	PD Section Header and No.
27	1. Each utility's Final Security Plan Report is due to the CPUC within 24 months of the approval of this decision.	38	6.6 Timeline for Implementation
28	2. POUs only — Within 30 months of the approval of this decision, POUs shall provide the CPUC with notice of the plan adoption by way of copy of signed resolution, ordinance or letter by a responsible elected- or appointed official, or utility director.	39	6.6 Timeline for Implementation
29	Utilities shall provide to the Director of the Safety and Enforcement Division and the Director of the Energy Division copies of OE-417 reports submitted to the U.S. DOE within two weeks of filing with U.S. DOE.	39	6.7 Reporting
30	We require the utilities to submit an annual report. These annual reports shall be submitted to the Director of the Safety and Enforcement Division and the Director of the Energy Division by March 31 of the following year. They shall report any physical security incidents resulting in any utility insurance claims, providing information on time and location of incident, impact on infrastructure, and amount of claim.	39	6.7 Reporting
31	These annual reports should also include any significant changes to the Security Plan Reports (including new facilities covered by the Plan or major mitigation upgrades at previously identified facilities). Because the statutory language provided that these be publicly available, the utility may provide both a complete report for the Commission and an appropriately redacted version for the public to be posted on the Commission's web site.	39	6.7 Reporting

No.	New Rule	Page No.	PD Section Header and No.
32	Utilities may establish a memorandum account to track associated costs. However, cost recovery requests shall be made in each utility's general rate case (GRC).	40	6.8 Cost Recovery
33	Electrical Cooperatives and POUs should act in accordance with processes established by a governing or other type of board with the authority to approve such processes, if any.	40	6.8 Cost Recovery
34	Phase I of this proceeding requires electric utilities to identify electric supply facilities which may require special protection and measures to identify risks and threats.	42	11. Conclusion
35	Each Operator will develop and implement a six-step Mitigation Plan modeled on the security plan requirements set forth by NERC CIP-014.	42	11. Conclusion
36	The safety and security benefits promoted by these Mitigation Plans mandate that the POUs also comply with these requirements as set forth in this decision.	42	11. Conclusion
37	9. Subsequent changes to the security plan requirements deemed beneficial and necessary, shall be enabled by one of the following: 1) Commission Resolution of Decision; 2) Ministerially, by SED (or successor entity) director letter.	40	Ordering Paragraph
38	29. An Exemption Request Process shall be available to utilities whose compliance would be clearly inappropriate or inapplicable or whose participation would result in an undue burden and hardship.	33, 36,49	Sec. 6.1, Ordering Paragraph, page footnote
	The Commission highly encourages and recommends the following optional security measures and best practices:		

No.	New Rule	Page No.	PD Section Header and No.
39	1. A training program for appropriate local law enforcement and utility security staff to optimize communication during a physical security event. Training for law enforcement should include information on physical infrastructure and relevant utility operations.	35	6.2.1 Additional Elective Measures for Mitigation Plans
40	2. A determination of the vulnerability of any associated communication utility infrastructure that supports priority distribution assets, which if deemed to be vulnerable, should have appropriate mitigation measures prescribed.	35	6.2.1 Additional Elective Measures for Mitigation Plans
41	3. Incorporating into applicable new and renovated or upgraded utility facilities design features that promote a sense of order and ownership, increase surrounding visibility and sightlines, capture opportunities for defensibility, and confound intrusion attempts by delaying and frustrating attackers via strategic placement of assets. These concepts, well-established within and -embraced by the power industry and other applications, are encouraged and called out by NERC within CIP-014 guidelines as Defense in Depth and Community Protection through Environmental Design.	35	6.2.1 Additional Elective Measures for Mitigation Plans