Physical Security of Electric Distribution Assets
California's Experience with Rulemaking to Address Grid Security
Transferable Lessons for States Contemplating Requirements Outside the Bulk Power System

By Jeremy Battis, Senior Analyst
Safety and Enforcement Division of the California Public Utilities Commission

A CPUC Staff White Paper for Presentation at the CRRI 32nd Western Conference
Monterey, California | June 2019

ABSTRACT

California became the first state to enact rules to safeguard the physical security of electric distribution assets in January 2019, when its Public Utilities Commission adopted Decision D.19-01-018,[1] requiring the State's electric utilities to submit completed physical security plans within 30 months for any assets deemed critical.[2]

The action was the culmination of a multiyear process[3] of fact finding, discovery, stakeholder engagement, and consensus building among affected electric utilities to establish new rules to safeguard California from the threat of terrorist attack on its power grid.

A CPUC staff inquiry component of that effort found California's existing distribution network to be fairly resilient, but nonetheless identified opportunities to enhance that resilience. With completion of the Commission's physical security rulemaking[4] effort, California and its electric utilities are well positioned to navigate a new era of heightened security risk. The Commission – via the rulemaking – established criteria for identifying critical distribution assets, and prescribed new procedures, measures, and mitigations[5] to advance the State's physical security goals. Many of these requirements and recommendations draw on electric-industry best practices and existing Federal-level rules, while others have their origins in behavioral sciences such as sociology and criminology, as will be described in this paper.[6]

---

[1] More at: http://docs.cpuc.ca.gov/SearchRes.aspx?docformat=ALL&DocID=260335905

[2] Broadly speaking, critical assets would be those that are indispensable to the utility performing its core function of operating its electrical grid or delivering power to a customer considered "essential" such as core public services and military user accounts. The definition generally employed at the Federal level is facilities that "if rendered inoperable or damaged could impact an interconnection through widespread instability, uncontrolled separation, or cascading failures."

[3] The proceeding was conducted within Order Instituting Rulemaking R.15-06-009, more at http://docs.cpuc.ca.gov/SearchRes.aspx?docformat=ALL&DocID=260335905

[4] As a quasi-legislative agency, the Commission is tasked with deriving codes and regulations that have the force of law.

[5] Mitigations, broadly speaking, are measures that reduce an identified risk to an acceptable level.

[6] This paper is an update to and overview of a more expansive CPUC staff white paper prepared in support of the Physical Security rulemaking. Readers seeking a more thorough treatment of the subject should review the earlier report at:

California's chosen approach represents a break from the prevailing industry response in the early years of the decade that favored hardening[7] of utility facilities as the appropriate means to secure against physical attacks. California's path forward leaves the door open for hardening of certain select electric utility assets that rise to a level considered critical[8] by means of a prescribed risk assessment and mitigation security-plan process. But for the vast majority of California distribution substations, the Commission found it more advantageous to rely on system redundancy and rapid repair of compromised assets through well-functioning supply chains of spare parts.

This Commission Staff Whitepaper surveys the process undertaken to bring a physical security rulemaking to a successful completion. The paper also shares key findings, takeaways, transferable lessons learned, and the outlook ahead as the State moves forward with carrying out the implementation phase.

KEY FINDINGS

California's distribution substations are numerous, are well dispersed, are generally assigned limited reach and responsibility, and are generally sited and employed to ensure some beneficial and deliberate redundancy.

Thus, the vast majority of distribution substations do not offer themselves as attractive or high-value targets; and

Thus, the vast majority of distribution substations do not hold value that would justify costly retrofit hardening measures. Additionally, it would be prohibitively expensive to harden and guard every distribution substation to a level that would reasonably defend against a coordinated attack.

Therefore, the best response to security threats for the majority of existing distribution substations, generally, is to support strategies to have failed assets quickly repaired, restored, and returned to service. Such supporting strategies would include having utilities:

- Enter into Mutual Assistance Agreements to provide aid to partner utilities in distress, and to coordinate within the industry to share information about operating conditions, challenges, and emerging and replicable methods and solutions;

https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/Final%20CPUC_Physical_Security_White_Paper_January_2018(1).pdf

[7] Hardening of assets such as distribution substations may include these typical measures: heavy high stone or concrete walls; thick and heavy steel plating shields to protect transformer hardware; razor wire and sharp dagger wall crowning; heavy entrance doors with advanced lock mechanisms; motion and gunshot detection technology; and high-resolution surveillance cameras.

[8] Facilities that if rendered inoperable or damaged could impact an Interconnection through widespread instability, uncontrolled separation, or cascading failures.

- Build rapport with, and exchange expertise and resources with local, State, and Federal law enforcement and regulatory authorities;
- Embrace an asset management program to promote optimization and quality assurance for tracking and locating spare parts stock to ensure availability and the rapid dispatch of available replacement hardware; and
- Support 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 across a utility's service territory

Having said this, there may be special circumstances that trigger exceptions. Consequently, there may be some limited number of distribution assets considered critical -- such as control centers or substations serving essential customers -- that merit prioritization and special resilience protection, which could include outright physical hardening.

KEY LEARNINGS

Electric utility staff may prove to be a valuable source of expertise on physical security practices and the Federal regulatory structure that informs much of the industry's approach to safeguarding critical assets.

Thus, utility staff can serve as pivotal partners in state-level physical security rule making proceedings.

Existing physical security rules at the Federal level[9] may serve as a good starting point for surveying and scoping a rulemaking.

State-level regulatory staff may wish to consider solicitation of an initial voluntary rule proposal from jurisdictional utilities as a starting point for assembling a set of new physical security rules.

A region's assigned Electric Reliability Organization[10] may be a rich source of expertise for state-level regulatory agencies seeking a qualified outside source for interpretations on existing Federal rules and procedures, opinions on proposed solutions, and appraisals of strengths and gaps among jurisdictional utilities.

Federal resources allocated to support utilities in gaining proficiency and coming into compliance with physical security rules are vast. The U.S. Department of Homeland Security

[9] More at: https://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx

[10] The ERO is the regional entity responsible for overseeing compliance of Federal-level physical security regulations. The ERO assigned to California and the western United States is the Western Electricity Coordinating Council. More at: https://www.nerc.com/pa/comp/Reliability%20Assurance%20Initiative/2018_ERO_CMEP_Implementation%20Plan_V2.1_May_2018.pdf

(U.S. DHS) offers or sponsors hands-on services that include facility and plan reviews and audits, and personnel training.[11]

KEY TAKEAWAYS

California's new rules for electric physical security are drawn from Federal requirements[12] and are built upon an effort by the State's electric utilities to draft new recommended rules outlined within a Joint Utility Proposal.[13]

In the course of new construction of or significant refurbishment of distribution substations and control centers, opportunities arise to incorporate low- to moderate-cost design features to discourage, delay, and frustrate a coordinated attack.

Accordingly, California electric utilities are required, within any new or renovated distribution substation, to incorporate reasonable security features within the facility.

Approaches for incorporating design features into existing and proposed facilities to increase their defensibility have gained credence in the power industry in recent decades. Such approaches seek to 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 approaches, endorsed by NERC, underlie the architecture-meets-behavioral concepts of *Defense in Depth* and *Crime Prevention through Environmental Design.*[14]

These concepts, because they increase resilience, may be appropriate for proposed new or refurbished substation facilities. Their specific design features include:

- Siting critical assets in a concentric manner such that a series of barriers must be breached, thereby providing an opportunity to delay and frustrate an attack;
- Positioning substation entrance and egress points such that they are consolidated and plainly visible; and
- Building and perimeter design features that promote a sense of order and project a strong sense of ownership and upkeep of the facility

[11] More at: https://www.dhs.gov/cisa/infrastructure-security

[12] Specifically, North America Electric Reliability Corporation (NERC) Critical Infrastructure Protocol (CIP)-014. More at https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-2.pdf

[13] Filed with the Commission August 31, 2017. More at: http://cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/R1506009-Updated%20Joint%20Straw%20Proposal%20and%20Cover%20083117%20Filing.pdf

[14] More at: https://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Physical%20Security%20Guideline%202011-10-21%20Formatted.pdf

Design features to increase resilience that may be appropriate for existing facilities include:

- Grading of earth to erect berms, removal of surrounding vegetation that may obscure sightlines and visibility, and installing perimeter fencing

AREAS OF SENSITIVITY AND POTENTIAL PITFALLS

Subject areas of the rulemaking that elicited resistance from utilities (and support from advocacy parties) pertained to the Commission's authority to:

- Direct utilities to provide the CPUC with highly-confidential data regarding physical security compliance (aka "highly-sensitive information"); and

- Assert jurisdiction and authority over California's publicly-owned utilities (POUs) for the purpose of ensuring public safety

On the first issue, the utilities' were adamant that all physical security plans and reports be considered highly-sensitive information, for which the utilities proposed to reserve sole custody of documentation and to make information available to CPUC staff upon request and at utility offices. The Commission, within Decision D.19-01-018,[15] ultimately determined that utility physical security plan compliance reports would be required to be submitted by the utilities to allow for independent viewing, appraisal, and retention by CPUC staff, oversight activities that are customary and necessary to carry out regulatory oversight responsibililty. CPUC staff requests for other physical security data outside of regularly-scheduled compliance filings would be subject to an interim reading room approach structured by utility staff on utility property.

On the second issue pertaining to POUs, the Commission ruled that it has complete and full jurisdiction and authority over California's publicly-owned utilities for the purpose of ensuring public safety, citing pertinent PU Code sections, General Orders, and case law established by California Supreme Court decisions.

RULEMAKING PROCESS

Following the Commission issuing an Order Instituting Rulemaking[16] in June 2015, to establish rules for the physical security of electric utilities, and a subsequent proceeding Scoping

[15] Commission Decision D.19-01-018, January 10, 2019, available at: http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=260335905

[16] Available at http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=152877601

Memo,[17] staff began planning a series of stakeholder workshops that broadly reflected recommendations received from interested parties during open comment periods.

To improve workshop programming, participation, and effectiveness, staff called for formation of a technical working group and convened the group of experts by hosting a series of conference calls. The working group, composed primarily of utility experts, aided in identifying and retaining expert speakers and venues for workshops.

Ultimately four workshops were held in three California regions and featured subject-matter-expert speakers representing NERC, the FBI, the U.S. DHS, and the Western Electricity Coordinating Council.

As ideas began to coalesce about appropriate approaches and solutions to inform new state-level physical security rules, Commission staff solicited a proposal from respondent utilities – California investor-owned; small, rural, and cooperative utilities, and publicly-owned utilities – for a set of new rules for CPUC consideration and to form the basis for a new state-level physical security framework.

California's electric utilities indicated a willingness to rise to the call and, in the summer of 2017, they initiated a months-long effort to draft a Joint Utility Proposal.[18]

Joint Utility Proposal

California's electric utilities collaborated to agree on terms and conditions to include within a straw proposal (or "utilities proposal") that outlined proposed new rules for physical security assessments and reports. Provisions included scope of assessments and reports, role of third-party reviewers, mitigation measures, and timelines.

The utilities' proposal was not as far-reaching as the Federal rules on which it was based. Rather, the utilities' submittal described consolidation of several discrete steps outlined under Federal rules. For instance, the utilities would not necessarily treat risk assessment, threat assessment, facility assessment, and security plan development as discrete tasks or phases. Also, Federal rules require third-party review at two intervals – once to review a draft risk assessment, and another to review a proposed set of mitigation measures. The utilities, by contrast, proposed a single mandatory third-party review step, which the Commission ultimately approved with some modifications.[19]

---

[17] More at: https://www.cpuc.ca.gov/uploadedFiles/CPUCWebsite/Content/Safety/Risk_Assessment/physicalsecurity/Scoping%20Physical%20Security%20031017.pdf

[18] See footnote No. 13, above.

[19] Two additional differences between Federal standards and the utilities' proposal were that: 1) Federal standards require a targeted security plan for each identified critical asset. The utilities' methodology by contrast, would complete one blanket security plan for all identified critical distribution assets; and 2) the utilities proposed to

One deficiency gap identified within the utilities' proposal was that it lacked a clear description of the role of the CPUC in the Security Plan process. Specifically, the utilities did not call out 1) CPUC plan-approval or -audit functions; or 2) how non-compliance would be dealt with by way of sanctions and penalties. Other omissions included 3) any mention of a mechanism to keep the CPUC informed via progress and incident reporting; and 4) a schedule for maintenance of utility security plans to make revisions at regular intervals. These four omissions were addressed by the CPUC in its Decision by:

1) Determining that the Commission would not perform a plan approver or auditor function, but instead would review[20] the plans to ensure that they were in compliance with regulatory requirements;

2) Affirming that utility non-compliance with the Commission's Decision orders could be met with sanctions and penalties;

3) Establishing that any Federally-mandated utility "incident" reports[21] submitted to the U.S Department of Energy to disclose irregularities such as power interruptions and physical- or cyber-attack are required to be provided to the Commission in a timely manner. Additionally, California utilities are required to provide the Commission with annual physical security reports that include a description of incidents that resulted in filing of an insurance claim; and

4) Mandating that California utilities must review any existing physical security plan or program every five years, and provide the Commission with a summary report of any program review activities and determination within 30 days of their completion

CPUC staff addressed the utility proposal in depth and made recommendations for modifications within a Staff Appraisal Response Document, published within a Ruling[22] issued by the assigned Administrative Law Judge.

---

approach the issue of physical security not by conducting a risk assessment for all distribution assets, but rather to begin by identifying a limited set of critical distribution assets, namely those necessary for restoring regional service and/or service to essential customers. The Commission approved these two aspects of the utilities' proposal with some modifications.

[20] To be more precise, review of plan reports will pertain to the State's IOUs. Publicly-owned utilities are required only to submit evidence that they have adopted a security plan. The CPUC's primary review task ahead for POU plan compliance will be to monitor their submittal of notice of plan adoption.

[21] The Federally-mandated incident report template, Form OE-417 Electric Disturbance Event, is now required to be provided to the Commission by California utilities within two weeks of notifying the U.S. DOE. More at: https://www.oe.netl.doe.gov/oe417.aspx

[22] *Safety and Enforcement Division's Risk Assessment & Safety Advisory staff evaluation of the Joint Utility Proposal and Recommendations for Consideration*, January 4, 2018 document, and January 16, 2018 ALJ Ruling available at: http://docs.cpuc.ca.gov/SearchRes.aspx?DocFormat=ALL&DocID=204350791 .

OUTLOOK AHEAD AND WHAT'S NEXT FOR CALIFORNIA

The next phase in California's effort to ensure the physical security of the distribution grid will be implementation and enforcement of the Commission Decision's requirements, the biggest part of which will be overseeing review of the California electric utilities' physical security plan reports[23] when they come due in summer 2021.

In the interim there exists an opportunity for the Commission to continue its dialogue on the subject of physical security with California's utilities at the staff level. Such communication may improve the compliance effort and could serve to promote information sharing and exchange of best practices across California and the utilities' service territories.

The physical security rulemaking process has the potential to have spillover benefits in the years ahead as it has deepened the Commission's understanding of the subject, which should prove valuable in the day to day work the CPUC does to carry out its safety and enforcement mandate. One opportunity would be the Commission's Safety RAMP process. The RAMP, or Risk Assessment Mitigation Phase,[24] is a mandated utility-safety compliance report required every three years. Broadly, the RAMP has the California IOUs[25] file organization-wide risk identification assessments that detail major safety threats accompanied by proposed mitigation measures, preferred-alternative plan proposals, and estimated program costs.[26]

California's three major electric IOUs have each completed a first-iteration RAMP report, outlining each utility's top risks. Within their RAMP reports, the IOUs have treated physical security inconsistently, sometimes including it as an identified risk meriting its own chapter focus, and in other instances dispersing the topic across related risk subjects such as insider threat. In instances where physical security has been identified as primary risk and assigned a focused RAMP chapter, informed reference to the physical security proceeding and Decision have not been referenced in the narrative. Going forward, in the course of reviewing future RAMP report iterations, CPUC staff can raise the issue of more consistent treatment of physical security in the utilities' RAMP reports, and encourage the utilities to have their RAMP reports reflect the of physical security proceeding and Decision.

A LOOK BACK AT EVENTS THAT LED TO THE COMMISSION'S ADOPTION OF DISTRIBUTION-LEVEL PHYSICAL SECURITY RULES

In the early morning of April 13, 2013, a sniper targeting PG&E's Metcalf Transmission Substation south of San Jose, fired 100 rounds of high-caliber ammunition, which resulted in approximately $15.4 million in damage.[27]

---

[23] Please see footnote No. 20 above for its clarification on the subject of plan review.
[24] More at https://www.cpuc.ca.gov/riskassessment/
[25] Investor owned-utilities
[26] A utility's RAMP report and staff review appraisal are required precursors to precede filing of a General Rate Case application, a process that also recurs every three years.
[27] Although PG&E initiated various changes to its security protocol, in late August 2014, burglars entered the Metcalf facility and removed tools and equipment valued at about $40,000.

Amid much nationwide speculation and rhetoric within industry, media, and political circles about the Metcalf attack representing a new grave and permanent domestic terrorist threat to the nation's power grid, the Federal government responded by updating the decade-old Critical Infrastructure Protocols (CIP). The new Federal rules were developed in a rulemaking conducted by the Federal Energy Regulatory Commission (FERC), and directed the North American Electric Reliability Corporation (NERC) to establish criteria for determining assets to be subject to new CIP rules. NERC completed the new rules (CIP-014) in May 2014 which under FERC auspices, established a uniform mandatory physical security standard for the nation's *transmission* assets, and required electric utilities to employ physical security plans to mitigate vulnerabilities within assets identified as critical.

In turn, in 2014, California State lawmakers responded by enacting SB 699,[28] which in amending Public Utilities Code Section 364, directed the Commission to appraise the NERC CIP rules to identify any perceived gaps in areas under CPUC jurisdiction; gaps with the potential to render the state's electric *distribution* facilities vulnerable. As discussed above, the Commission's gap analysis was limited to distribution assets over which Federal jurisdiction does not extend. Areas for improvement identified were addressed as new mandatory program efforts to guide an asset security-plan assessment process, robust spare parts and repair procedures, and policies to ensure that future substations are designed to deter and frustrate a physical attack.

Disclaimer

This Report was prepared by California Public Utilities Commission (CPUC) staff. It does not necessarily represent the views of the CPUC, its Commissioners, or the State of California.

The CPUC, the State of California, its employees, contractors, and subcontractors make no warrants, express or imply, and assume no legal liability for the information in this Report.

This Report has not been approved or disapproved by the CPUC.

[28] More at: https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201320140SB699

Attachment A

DECISION D.19-01-018 PHYSICAL SECURITY REQUIREMENTS

Six-step Process for Electric Utility Physical Security Plan Compliance

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.

Step 2. Independent Review and Utility Response to Recommendations. Proposed plan would be reviewed 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.

Step 3. SED Review (for IOUs only). Final plan report would be reviewed by the CPUC SED (recurring every five years)[29] so as to determine whether it is in compliance with regulatory requirements, and eligible to request funding for implementation. Upon five years from the date of adoption, a utility would be required to have any revised or original plan updated and repeat the review process. Utilities may be afforded regulatory relief by way of an exemption request process for special cases where undertaking of the plan overhaul and/or review process may be impracticable or unduly burdensome. Non-compliance could result in an enforcement action, potentially resulting in sanctions and/or penalties as provided by PU Code Sec. 364(c). An SED finding of compliance would render IOUs eligible to request funding for appropriate physical security needs identified by IOUs; project expenditures would be tracked in a memorandum account and subject to reasonableness review in the GRC.

Step 3a. Plan Review (for POUs only). Final plan report would be deemed adequate (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.)

[29] This time interval is based on the requirements instituted for the City of Los Angeles under City Charter.

Step 4. Adoption (for POUs only). Reviewed 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.

Step 4a. Notice. (for POUs only). Provide CPUC with official notice (ideally including a copy of a resolution of the adopted plan action.

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.

Step 6. Repeat Process. Plan overhaul and review every five years.

Ordering Paragraphs

IT IS ORDERED that:

1. Within 18 months of this decision being adopted, Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall prepare and submit to the Commission a preliminary assessment of priority facilities for their distribution assets and control centers.
2. Within 30 months of this decision being adopted, Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall submit each utility's Final Security Plan Report.
3. Within 30 months of this decision being adopted, the Publicly Owned Utilities shall provide the Commission with notice of final plan adoption.
4. The Publicly Owned Utilities' notice of final plan adoption may consist of a copy of a signed resolution, ordinance or letter by a responsible elected- or appointed official, or utility director.
5. All California Electric Utility Distribution Asset Physical Security Plans shall conform to the requirements outlined within the Joint Utility Proposal, as modified by this decision (rules and requirements collectively known as "security plan requirements").
6. The Investor Owned Utilities and Publicly Owned Utilities shall adhere to the Safety and Enforcement Division's Six-step Security Plan Process.
7. The Six-step Plan Process consists of the following: Assessment; Independent Review and Utility Response to Recommendations; Safety and Enforcement Division Review (for

Investor Owned Utilities s); Local Plan Review (for Publicly Owned Utilities); Maintenance and Plan overhaul/new review.

8. Subsequent changes to the security plan requirements deemed beneficial and necessary, shall be enabled by one of the following: 1) Commission Resolution or Decision; 2) Ministerially, by Safety and Enforcement Division (or successor entity) director letter.

9. In carrying out any future changes to the security plan requirements, Safety and Enforcement Division shall confer with utilities about any recommended modifications to the plan requirements.

10. Prior to the submittal of the Security Plan, Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall each have their respective plan reviewed by an unaffiliated third-party entity.

11. The unaffiliated third-party reviewer shall have demonstrated appropriate physical security expertise.

12. California electric utilities shall, within any new or renovated distribution substation, design their facilities to incorporate reasonable security features.

13. Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement 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.

14. Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement 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.

15. Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement a preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately.

16. Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement a description of Distribution Control Center and Security Control Center roles and actions related to distribution system physical security.

17. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall each

document all third-party reviewer recommendations, and specify recommendations that were accepted or declined by the utility.

18. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall each provide justification supporting its decision to accept or decline any third-party recommendations.

19. Physical Security-related information is bifurcated into two categories. Recurring and routine utility compliance work products and ongoing utility updates required by this decision are not subject to the Reading Room approach but shall be transmitted to the Commission. All other physical security data requested by Commission staff on an ad hoc basis shall be made available to the Commission on utility property in a manner agreed to by the Safety and Enforcement Division, or its successor, until such time that the Commission finalizes its rules for the handling, sharing, and inspection of confidential information.

20. If a Publicly Owned Utility has an existing blanket Security Plan that has been adopted by its Board of Directors or City Council within three years prior to the date of this decision, the requirement to have a plan adopted may be waived by the Commission.

21. In the event that a Publicly Owned Utility's (POU) Security Plan has not been adopted in time as required by this decision, the POU shall provide the Director of the Commission's Safety and Enforcement Division with a notice [30] days prior to the deadline with information on the nature of the delay and an estimated date for adoption.

22. Prior to Security Plan adoption, Publicly Owned Utilities in California shall have their plan reviewed by a third party.

23. Such third-party reviewer may be another governmental entity within the same political subdivision, so long as the entity can demonstrate appropriate expertise, and is not a division of the publicly owned utility that operates as a functional unit (*i.e.,* a municipality could use its police department if it has the appropriate expertise).

24. Publicly Owned Utilities shall conduct a program review of their Security Plan and associated physical security program every five years after initial approval of the Security Plan by their Board of Directors or City Council. Notice of such approval action shall be provided to the Commission's Safety and Enforcement Division within 30 days of Plan

adoption by way of copy of signed resolution or letter by a responsible elected- or appointed official, or utility director.

25. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall conduct a program review of their Security Plan and associated physical security program every five years after Commission review of the first iteration of the Security Plan.

26. A summary of the program review shall be submitted to the Safety and Enforcement Division within 30 days of review completion.

27. In the event of a major physical security event that impacts public safety or results in major sustained outages, all utilities shall preserve records and evidence associated with such event and shall provide the Commission full unfettered access to information associated with its physical security program and the circumstances surrounding such event.

28. 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.

29. Utilities shall provide to the Director of the Safety and Enforcement Division and Energy Division copies of OE-417 reports submitted to the United States Department of Energy (U.S. DOE) within two weeks of filing with U.S. DOE.

30. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco (collectively, IOUs) shall seek recovery of costs associated with their respective Distribution Security Programs in each IOU's general rate case.

31. The utilities shall submit an annual report by March 31 each year beginning 2020, reporting physical incidents that result in any utility insurance claims, providing information on incident, location, impact on infrastructure and amount of claim. The insurance claim disclosure reporting, as described in this decision, should be included within a utility's broader annual Physical Security Report to the Commission due every March 31, beginning in 2020.

32. As appropriate, the requirements set forth in Phase I of this proceeding shall apply to Alameda Municipal Power, City of Anaheim Public Utilities Department, Azusa Light and Water, City of Banning Electric Department, Biggs Municipal Utilities, Burbank Water and

Power, Cerritos Electric Utility, City and County of San Francisco, City of Industry, Colton Public Utilities, City of Corona, Eastside Power Authority, Glendale Water and Power, Gridley Electric Utility, City of Healdsburg Electric Department, Imperial Irrigation District, Kirkwood Meadows Public Utility District, Lathrop Irrigation District, Lassen Municipal Utility District, Lodi Electric Utility, City of Lompoc, Los Angeles Department of Water & Power, Merced Irrigation District, Modesto Irrigation District, Moreno Valley Electric Utility, City of Needles, City of Palo Alto, Pasadena Water and Power, City of Pittsburg, Port of Oakland, Port of Stockton, Power and Water Resources Pooling Authority, Rancho Cucamonga Municipal Utility, Redding Electric Utility, City of Riverside, Roseville Electric, Sacramento Municipal Utility District, City of Shasta Lake, Shelter Cove Resort Improvement District, Silicon Valley Power, Trinity Public Utility District, Truckee Donner Public Utilities District, Turlock Irrigation District, City of Ukiah, City of Vernon, Victorville Municipal Utilities Services, Anza Electric Cooperative, Plumas-Sierra Rural Electric Cooperative, Surprise Valley Electrification Corporation, and Valley Electric Association.

33. This proceeding shall remain open so that the Commission may address the issues presented in Phase II of this proceeding.

This order is effective today.

Dated January 10, 2019, at San Francisco, California.