FILED
8-31-17
04:59 PM

**BEFORE THE PUBLIC UTILITIES COMMISSION OF THE**

**STATE OF CALIFORNIA**

| | |
|---|---|
| Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electrical Corporations Consistent with Public Utilities Code Section 364 and to Establish Standards for Disaster and Emergency Preparedness Plans for Electrical Corporations and Regulated Water Companies Pursuant to Public Utilities Code Section 768.6. | Rulemaking 15-06-009<br>(Filed June 11, 2015) |

# JOINT PARTIES' FILING OF UPDATED DRAFT STRAW PROPOSAL FOR PHYSICAL SECURITY REGULATIONS


GLORIA ING
ROBERT KANG

Attorneys for
SOUTHERN CALIFORNIA EDISON COMPANY

2244 Walnut Grove Ave.
Rosemead, CA 91770
Telephone: (626) 302-6012
Facsimile: (626) 302-1935
Email: Robert.Kang@sce.com


Dated: **August 31, 2017**

**BEFORE THE PUBLIC UTILITIES COMMISSION OF THE**

**STATE OF CALIFORNIA**

| | |
|---|---|
| Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electrical Corporations Consistent with Public Utilities Code Section 364 and to Establish Standards for Disaster and Emergency Preparedness Plans for Electrical Corporations and Regulated Water Companies Pursuant to Public Utilities Code Section 768.6. | Rulemaking 15-06-009<br>(Filed June 11, 2015) |

# JOINT PARTIES' FILING OF UPDATED DRAFT STRAW PROPOSAL FOR PHYSICAL SECURITY REGULATIONS

## I.

## INTRODUCTION

Southern California Edison Company ("SCE") and the parties listed below submit the attached updated straw proposal in response to the Administrative Law Judge's July 12, 2017 Ruling, as amended by the Administrative Law Judge's e-mail ruling of August 24, 2017. This proposal is submitted jointly by SCE and by the parties listed below.[1]

The attached straw proposal merges the two proposals submitted to the Commission on June 20, 2017, and includes input obtained at workshops led by the California Public Utilities Commission's Safety & Enforcement Division staff ("Commission" and "SED," respectively).

The parties appreciate this opportunity to work on this issue of common interest, and look forward to working collaboratively with the Commission.

[1] SCE counsel represents that the parties listed below authorized SCE to join in this filing.

**The following parties join in submitting the proposal:**

- Bear Valley Electric Service
- California Municipal Utilities Association ("CMUA")
- Los Angeles Department of Water & Power ("LADWP")
- Liberty CalPeco
- National Rural Electric Cooperative Association ("NRECA")
- PacifiCorp
- Pacific Gas & Electric Company
- Sacramento Municipal Utility District ("SMUD")
- San Diego Gas & Electric Company
- Southern California Edison Company

## II.

## JURSIDCTIONAL STATEMENT OF THE CALIFORNIA MUNICIPAL UTILITIES ASSOCIATION, LOS ANGELES DEPARTMENT OF WATER & POWER, NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION, AND SACRAMENTO MUNICIPAL UTILITY DISTRICT[2]

The legislative mandates included in SB 699 (stats. 2014) and AB 1650 (stats. 2012) are specific to Commission-jurisdictional entities and, as a result, local publicly owned electric utilities ("POUs") do not fall within the scope of this rulemaking and are not subject to the Commission's enforcement jurisdiction.[3] CMUA members, including SMUD and LADWP, are owners and operators of transmission and distribution facilities located in the State of California and appreciate the importance of the issues raised in the rulemaking. For that reason, CMUA, SMUD, and LADWP are parties to this proceeding, and have participated in the workshops and working groups to develop reasonable industry guidelines based on best practices. CMUA,

---

[2] This Jurisdictional Statement is included in this filing on behalf of CMUA, LADWP, NRECA and SMUD, and as a convenience for the Commission by consolidating initial comments about the Joint Proposal into a single filing. The other parties referenced in Section I of this filing, including the filing party, take no position on the Jurisdictional Statement.

[3] See Opening Comments of The Los Angeles Department of Water and Power, dated July 22, 2015, at 2-6.

SMUD, and LADWP object to the Commission's assertion of jurisdiction to impose and enforce rules on the POUs governing the electric transmission and distribution systems of POUs. CMUA, SMUD, and LADWP's participation in this proceeding, including joining the submission of this Straw Proposal, does not waive this jurisdictional issue. Any decision, ruling, or order adopted in this proceeding should be consistent with the legislative mandate set forth in SB 699 and the amendments to Public Utilities Code section 364, as well as AB 1650 and Public Utilities Code Section 768.6, and will not expand or enlarge the Commission's jurisdiction over POUs.

Further, the Commission's jurisdiction over Electrical Cooperatives is limited under Public Utilities Code section 2777. The Electrical Cooperatives have participated in this proceeding for similar reasons as the POUs and do not concede or waive jurisdiction through their participation in this proceeding.

Respectfully submitted,

GLORIA ING
ROBERT KANG

*/s/ Robert Kang*
By: Robert Kang

2244 Walnut Grove Ave.
Rosemead, CA 91770
Telephone: (626) 302-6012
Facsimile: (626) 302-1935
Email: Robert.Kang@sce.com

August 31, 2017

Attorneys for
Southern California Edison Company

ATTACHMENT

**STRAW PROPOSAL**
**R.15-06-009**
**Proposed Guidelines for Electric Utility Distribution System Security Assessments**

# PART 1
# INTRODUCTION

## 1 Purpose

The purpose of these guidelines is to address the physical security risks to the distribution systems of Electrical Corporations, in compliance with Senate Bill 699 (Ch. 550, Hill), as codified at California Public Utilities Code Section 364.

## 2 Applicability

The guidelines contained in this proposal apply to Electrical Corporations subject to the jurisdiction of the California Public Utilities Commission (Commission). These guidelines do not apply to the Local Publicly Owned Electric Utilities and Electrical Cooperatives, however, they represent industry standards that the POUs and electrical cooperatives will use to evaluate and update their current physical security programs, subject to the oversight of their respective governing bodies.

These guidelines do not apply to facilities subject to the California Independent System Operator's operational control and/or subject to North American Electric Reliability Corporation (NERC) Reliability Standard CIP-014-2 or its successors.

## 3 General

This document is intended to implement a risk management approach towards distribution system physical security, with appropriate consideration for the resiliency, impact, and cost.

This document reflects the following general principles, as established in the workshops:

- Distribution systems are not subject to the same physical security risks and associated consequences, including threats of physical attack by terrorists, as the transmission system.
- Distribution utilities will not be able to eliminate the risk of a physical attack occurring, but certain actions can be taken to reduce the risk or consequences, or both, of a significant attack.
- A one-size-fits-all standard or rule will not work. Distribution utilities should have the flexibility to address physical security risks in a manner that works best for their systems and unique situations, consistent with a risk management approach.

- Protecting the distribution system should consider both physical security protection and operational resiliency or redundancy.
- The focus should not be on all Distribution Facilities, but only those that risk dictates would require additional measures.
- Planning and coordination with the appropriate federal and state regulatory and law enforcement authorities will help prepare for attacks on the electrical distribution system and thereby help reduce or mitigate the potential consequences of such attacks.

## PART 2
## DEFINITIONS

**Confidential Information**: Information that the Commission determines is exempt from the California Public Records Act. Such information may be submitted to the Commission pursuant to Public Utilities Code Sections 364(d) and 583.

**Covered Distribution Facility:** A Distribution Facility, resulting from the process set forth in Part 3.

**Distribution Control Center**: a facility that has responsibility for monitoring and directing operational activity on distribution power lines and Distribution Substations.

**Distribution Facility:** A Distribution Substation or Distribution Control Center.

**Distribution Substation**: an electric power substation associated with the distribution system and the primary feeders for supply to residential, commercial, and/or industrial loads.

**Electrical Cooperative:** as defined in California Public Utilities Code Section 2776.

**Electrical Corporation:** as defined in California Public Utilities Code Section 218.

**Local Publicly Owned Electric Utility**: as defined in California Public Utilities Code Section 224.3.

**Mitigation Plan:** The documentation of a risk-based strategy for mitigating the impacts of a physical attack on a Covered Distribution Facility. The strategy may consist of operational resiliency measures or physical security measures.

**Operator**: an Electrical Corporation, a Local Publicly Owned Electric Utility, or an Electrical Cooperative responsible for the reliability of one or more Distribution Facilities.

**Public Information:** Information that can be made publicly available in accordance with the California Public Records Act and without causing negative impacts to customer and utility safety, security, reliability, privacy and/or economics.

**Reading Room Approach:** A method for sharing Security-Sensitive Information with the Commission. Security-Sensitive Information will be available for inspection at the Operator's headquarters, or a mutually agreed-to location, by Commission staff upon request.

**Security-Sensitive Information:** Information that if disclosed could negatively impact public safety or the safe and reliable operation of an Operator's system. Such information may only be shared with Commission staff using enhanced access controls, such as the Reading Room approach. Such information is exempt from the California Public Records Act.

## PART 3
## DISTRIBUTION SUBSTATION & DISTRIBUTION CONTROL CENTER SECURITY PROGRAMS

### 1. Overview

Each Operator will establish a Distribution Substation and Distribution Control Center Security Program (Distribution Security Program).

As part of its Program, each Operator will identify which, if any, of its Distribution Facilities meet the criteria set forth in Section 2 of this Part.

Next, the Operator, pursuant to Section 3 of this Part, will evaluate the potential risks associated with a physical attack on each of the Distribution Facilities meeting the criteria of Part 3, Section 2, and assess whether existing grid resiliency and/or physical security measures appropriately mitigate the risks. Those identified Distribution Facilities that do not have existing grid resiliency and/or physical security measures necessary to appropriately mitigate the risks will be considered Covered Distribution Facilities.

For each of its Covered Distribution Facilities, an Operator will then develop a Mitigation Plan to document the strategy for mitigating the risk and/or consequences of an attack on the Covered Distribution Facility.

An unaffiliated third-party will review (1) the process used by Operators to identify the Covered Distribution Facilities and (2) the Mitigation Plan(s) developed by Operators to reduce the risks and/or the consequences of an attack on Covered Distribution Facilities.

Each Operator will review each of its Mitigation Plans at least once every five years.

### 2. Identification

Consistent with the general principles in Part 1, Section 3, the following criteria provide Operators with guidance needed to identify Distribution Facilities requiring further assessment:

a) Distribution Facility necessary for crank path, black start or capability essential to the restoration of regional electricity service that are <u>not</u> subject to the California

Independent System Operator's (CAISO) operational control and/or subject to North American Electric Reliability Corporation (NERC) Reliability Standard CIP-014-2 or its successors;

b) Distribution Facility that is the primary source of electrical service to a military installation essential to national security and/or emergency response services (may include certain air fields, command centers, weapons stations, emergency supply depots);
c) Distribution Facility that serves installations necessary for the provision of regional drinking water supplies and wastewater services (may include certain aqueducts, well fields, groundwater pumps, and treatment plants);
d) Distribution Facility that serves a regional public safety establishment (may include County Emergency Operations Centers; county sheriff's department and major city police department headquarters; major state and county fire service headquarters; county jails and state and federal prisons; and 911 dispatch centers);
e) Distribution Facility that serves a major transportation facility (may include International Airport, Mega Seaport, other air traffic control center, and international border crossing);
f) Distribution Facility that serves a Level 1 Trauma Center as designated by the Office of Statewide Health Planning and Development;
g) Distribution Facility that serves over 60,000 meters.

If an Operator does not identify any Distribution Facilities requiring further assessment, the Operator is not required to conduct the tasks set forth in Part 3, Sections 3, 4, 5 and 7.

**3. Assessment**

Once an Operator has identified its Distribution Facilities that require further assessment taking into account the criteria described in Part 3, Section 2, the Operator will conduct an evaluation of the potential risks associated with a successful physical attack on such Facilities and whether existing grid resiliency, requirements for customer-owned back-up generation and/or physical security measures appropriately mitigate the risks. In conducting this evaluation, the Operator may consider, without limitation, the following factors:

- The existing system resiliency and/or redundancy solutions (e.g., switching the load to another substation or circuit capable of serving the load, temporary circuit ties, mobile generation and/or storage solutions);
- The availability of spare assets to restore a particular load;
- The existing physical security protections to reasonably address the risk;
- The potential for emergency responders to identify and respond to an attack in a timely manner;
- Location and physical surroundings, including proximity to gas pipelines and geographical challenges, and impacts of weather;
- History of criminal activity at the Distribution Facility and in the area.
- The availability of other sources of energy to serve the load (e.g., customer-owned back-up generation or storage solutions);

- The availability of alternative ways to meet the health, safety, or security requirements served by the load (e.g., back up command center or water storage facility).

Those Distribution Facilities whose risks are not appropriately mitigated through existing grid resiliency and/or physical security measures are Covered Distribution Facilities subject to the measures set forth in Part 3, Section 4.

## 4. Mitigation Plan

Each Operator will develop and implement a Mitigation Plan to address the potential risks associated with a physical attack on its respective Covered Distribution Facilities.

The Operator has discretion to select the specific security measures or resiliency solutions it deems most appropriate for each Covered Distribution Facility. The Mitigation Plan will include consideration of the reasonableness of the cost of any recommended physical security improvements or resiliency solutions. The Operator may also consider local geography and weather, applicable codes (such as the National Electrical Safety Code then in effect), national electrical industry practices, sound engineering judgment, and its own experience. The primary focus of the Mitigation Plan is to specifically address the risk of a long-term outage to a Covered Distribution Facility due to a physical attack.

In developing the Mitigation Plans, Operators may use risk-based performance standards to identify the means by which a Covered Distribution Facility's security can be upgraded (e.g., perimeter security, improved monitoring) and its resiliency improved (e.g., timely access to spare equipment, the ability to serve in whole or in part from another facility or circuit, back-up generation or storage). A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the Operator. In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance standard sets a goal, which in this case is to reduce the risk and/or consequences of a successful physical attack on a Covered Distribution Facility, and provides for a variety of solutions to mitigate the risk and/or consequences and achieve the goal.

The following are illustrative examples of potential resiliency and security solutions that could be deployed to address identified risks and are not meant to be binding or definitive or to be required for any particular Distribution Facility:

<u>Examples of Potential Resiliency Solutions</u>

(a) Strategically Located Spares – Strategically locate spare equipment to facilitate the repair of a Covered Distribution Facility;
(b) Distribution Resiliency Upgrades – Adding circuit ties or other facilities to enhance the ability to switch around damaged facilities to facilitate the repair and restoration of service;

(c) Enhanced Resiliency Response – Develop response strategies for temporarily restoring service (e.g., mobile generation/storage, jumper from an adjacent circuit);

Examples of Potential Security Solutions

(a) Access – Measures to limit unauthorized entry or breach of the facility (e.g., fencing, gates, barriers or other security devices);

(b) Deterrent – Measures to discourage unauthorized entry or breach of the facility (e.g., cameras, lights);

(c) Coordination – Measures to further collaborate with Law Enforcement as appropriate.

## 5. Verification

Each Operator will select an unaffiliated third party with the appropriate experience needed to review the Identification and Assessment evaluations and the Mitigation Plan(s) performed and developed by said Operator under Part 3, Sections 2, 3, and 4. This review may occur concurrently with or after the development of the Mitigation Plan, pursuant to the Operator's Distribution Security Program. Each Operator will either modify its Mitigation Plan consistent with the recommendation, if any, of the reviewer, or document its reasons for not doing so. Any Operator that has not identified any Distribution Facilities requiring further assessment pursuant to Part 3, Section 2, is not obligated to meet the requirements of this Section 5.

## 6. Records

Electronic or hard copy records of the Operator's Distribution Security Program implementation will include, at a minimum:

- The Operator's Identification of Distribution Facilities requiring further assessment under Section 2.
- Each Operator's Assessment of the potential threats and vulnerabilities of a physical attack and whether existing grid resiliency, customer-owned back-up generation and/or physical security measures appropriately mitigate the risks on each of its identified Distribution Facilities under Section 3.
- Each Operator's Mitigation Plans covering each of its Covered Distribution Facilities under Section 4.
- The unaffiliated third-party evaluation of the Operator's Identification and Assessment evaluations and Mitigation Plans performed and developed by the Operator under Sections 2, 3, and 4.
- If applicable, the Operator's documented reasons for not modifying its Mitigation Plans consistent with the unaffiliated third-party's evaluation.

Electronic or hard copy records of the Distribution Security Program implementation will be retained for not less than five (5) years.

Records maintained under this Part are extremely confidential and will be maintained in a secure manner at the Operator's headquarters. The records maintained by Electrical Corporations will be available for inspection at the Electrical Corporations' headquarters or San Francisco offices by Commission staff upon request.

## 7. Timelines and Frequency

Any Operator that has identified at least one Distribution Facility requiring further assessment pursuant to Part 3, Section 2 whose risks are not found to be appropriately mitigated after the assessment under Part 3, Section 3, will complete an initial draft of its Mitigation Plan(s), described in Section 4, within eighteen (18) months from the effective date of these guidelines.

Where the Operator is required to seek verification pursuant to Part 3, Section 5, the Operator will obtain an unaffiliated, third-party review, described in Part 3, Section 5, within twenty-seven (27) months from the effective date of these guidelines. Each Operator will meet its obligations, described in Sections 4 and 5 within thirty (30) months of the effective date of these guidelines.

## 8. Cost Recovery

At its discretion, the Operator may establish an account to track the expenditures associated with the development and execution of its Distribution Security Program. Electrical Corporations are authorized to file Tier 1 Advice Letters for this purpose. Electrical Cooperatives and Local Publicly Owned Electric Utilities should act in accordance with processes established by a governing or other type of board with the authority to approve such processes, if any.

The Electrical Corporations are also authorized to file separate applications or GRC requests for the recovery of costs associated with their respective Distribution Security Programs. Although the Distribution Security Program documents are considered Security-Sensitive Information and cannot be filed as supporting documentation, the Electrical Corporations may file a public version of the unaffiliated third-party review and Commission approval in support of their recovery requests.

# PART 4
# VERIFICATION REVIEW

The Commission may review the unaffiliated third-party verification performed pursuant to an Electrical Corporation's Distribution Security Program to determine such verification was performed in accordance with Part 3, Section 5. Because the documents developed as part of a Distribution Security Program are considered to be Security-

Sensitive Information (described in Part 5), the review would take place at the Electrical Corporation's headquarters or another facility mutually-agreed upon that can be adequately secured for the purpose of sharing Security-Sensitive Information.

For Local Publicly Owned Electrical Utilities and Electrical Cooperatives, the governing board of the Local Publicly Owned Electrical Utility or Electrical Cooperative may review or establish a process for review of the third-party verification to determine such verification was performed in accordance with Part 3, Section 5.

## PART 5
## ELECTRICAL CORPORATION INFORMATION SHARING PROTOCOLS

There will be three designated sensitivity levels for Electrical Corporation distribution system information and the following information sharing protocols will apply for each respective level:

**Public Information (defined above):** Information that can be made publically available in accordance with the California Public Records Act and without causing negative impacts to customer and utility safety, security, reliability, privacy and/or economics. The Operators propose no additional changes for how this information is transmitted or secured.

**Confidential Information (defined above)**: Information that the Commission determines is exempt from the California Public Records Act. Such information may be submitted to the Commission pursuant to Public Utilities Code Sections 364(d) and 583. The Operators propose no additional changes for how this information is transmitted or secured.

**Security-Sensitive Information (defined above):** Information that is exempt from the California Public Records Act, and which may be shared with Commission staff only using enhanced secure access control measures, such as the Reading Room approach. Disclosure of Security-Sensitive Information could negatively impact public safety or the safe and reliable operation of an Operator's system, and will be shared only when using heightened security controls beyond Public Utilities Code Section 583.

The definition of Security-Sensitive Information and proposal for how it is transmitted and secured was developed as a direct result of security expert panel discussions, Operator and stakeholder presentations, as well as input and comments from the CPUC.