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.	R._____

ORDER INSTITUTING RULEMAKING TO FULFILL THE REQUIREMENTS OF PUBLIC UTILITIES CODE SECTIONS 364 AND 768.6

Table of Contents

Title **Page**

ORDER INSTITUTING RULEMAKING TO FULFILL THE REQUIREMENTS OF PUBLIC UTILITIES CODE SECTIONS 364 AND 768.6 1
Summary 2
1. Events Leading to Senate Bill (SB) 699 2
   1.1 Changes to Public Utilities Code Section 364 4
   1.2. Applicable Safety Standards Prior to the Amendment of Section 364 of the Public Utilities Code 5
   1.3. Discussion Pertaining to SB 699 8
2. Events Leading to Assembly Bill (AB) 1650 9
   2.2. Emergency and Disaster Preparedness Plans for Electrical Corporations and Regulated Water Corporations Prior to the Addition of Public Utilities Code Section 768.6 13
   2.3. Discussion Pertaining to AB 1650 14
3. Preliminary Scope 15
   3.1. Issues to be Considered Pursuant to SB 699 15
   3.2. Issues to be Considered Pursuant to AB 1650 16
4. Preliminary Schedule and Initial Comments 17
5. Proceeding Category and Need for Hearing 18
6. Respondents 19
7. Service of OIR 19
8. Filing and Service of Comments and Other Documents 21
9. Addition to Official Service List 21
10. Subscription Service 22
11. Public Advisor 22
12. Intervenor Compensation 22
13. *Ex Parte* Communications 23

Appendix A - Senate Bill 699 amending Public Utilities Code Section 364
Appendix B - Regulation of Physical Security for the Electric Distribution System, February 2015
Appendix C - Assembly Bill 1650 adding Public Utilities Code Section 768.6
Appendix D - California Publicly Owned Electric Utilities
Appendix E - List of Rural Electric Cooperatives

Table of Contents (cont.)

Title **Page**

Appendix F - Publicly Owned Utilities Representatives and Agents
Appendix G - Facilities-Based Communications Carriers Authorized to Operate in California
Appendix H – Service List of Resolution No. W-4823

ORDER INSTITUTING RULEMAKING TO FULFILL THE REQUIREMENTS OF PUBLIC UTILITIES CODE SECTIONS 364 AND 768.6

Summary

This rulemaking is opened to establish policies, procedures, and rules for the regulation of physical security risks to the electric supply facilities of electrical corporations consistent with Public Utilities Code Section 364.[1]

This rulemaking is also opened to establish standards for disaster and emergency preparedness plans for electrical corporations and regulated water companies consistent with Public Utilities Code Section 768.6.[2]

We will consider whether any new rules, standards, or General Orders (GO) or modifications to other existing policies should apply to all electrical supply facilities within the jurisdiction of the Commission, including facilities owned by publicly-owned-utilities, rural electric cooperatives and regulated water companies. This proceeding will be conducted in phases. The first phase will pertain to the requirements to address the physical security risks to the electrical supply facilities of electrical corporations. Additional phases will be conducted to address emergency and disaster preparedness plans of electrical corporations and regulated water companies.

1. Events Leading to Senate Bill (SB) 699

The vulnerability of electrical supply facilities has been demonstrated in recent years by attacks. In April 2013, a rifle attack occurred at Pacific Gas and

---

[1] Section 364 of the Public Utilities Code was amended by Senate Bill 699 (Stats. 2014, ch. 550, Sec. 2).

[2] Section 768.6 of the Public Utilities Code was added by Assembly Bill 1650 (Stats. 2012, ch. 472).

Electric's (PG&E) Metcalf Transmission Substation south of San Jose, resulting in approximately $15.4 million in damages. Although PG&E initiated various changes in its security protocol, in late August 2014, burglars entered the Metcalf facility and removed $38,651 of tools and equipment.[3]

Regulatory jurisdiction over transmission facilities and substations is shared between federal and state agencies. The Federal Energy Regulatory Commission (FERC) is an independent federal agency that regulates the interstate transmission of electricity, including the "Bulk-Power System" and related facilities that include some high voltage transmission facilities and substations.[4]

Several grid security guidelines or standards have been proposed or developed to address the physical security of the electrical supply facilities of electrical corporations. However, prior to the Metcalf incident, many of these standards were considered as voluntary best practices. Following the Metcalf incident, FERC ordered the imposition of mandatory physical security standards to be prepared by the North American Electric Reliability Corporation (NERC).[5] In California, SB 699 was enacted to ensure that steps would be taken to reasonably protect electrical supply facilities of electrical corporations against further attacks.[6]

---

[3] PG&E. *Metcalf Root Cause Analysis Summary Report*. November 21, 2014 at 2.

[4] Http://www.ferc.gov.

[5] NERC is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. See, http://www.nerc.com.

[6] The Commission does not expect anything in this rulemaking to conflict with any FERC or NERC regulations, jurisdiction, or proceedings.

1.1 Changes to Public Utilities Code Section 364

SB 699 amended Section 364 of the Public Utilities Code to require that the Commission "in a new proceeding, or new phase of an existing proceeding, to commence on or before July 1, 2015, consider adopting rules to address the physical security risks to the distribution systems of electrical corporations." Additionally, this legislation provides that the Commission may, "consistent with other provisions of law, withhold from the public information generated or obtained pursuant to this section that it deems would pose a security threat to the public if disclosed." This rulemaking is concerned with implementing the amendments to Section 364 of the Public Utilities Code.

Prior to SB 699, Section 364 of the Public Utilities Code provided the following.

1. Requires the Commission to adopt inspection, maintenance, repair, and replacement standards for the distribution facilities of investor-owned utilities (IOUs) in order to provide high-quality, safe, and reliable service.
2. Requires the Commission to adopt standards for operation, reliability, and safety during periods of emergency and disaster.
3. Requires each utility to report annually on compliance with the applicable standards.
4. Requires annual compliance reports submitted by the utility to be made available to the public.
5. Requires the Commission to conduct a review to determine whether the standards have been met and to perform a review after every major outage.
6. Provides that the Commission may order appropriate sanctions, "including penalties in the form of rate reductions or monetary fines."

7. Any penalties or fines collected shall be used to offset funding for the California Alternative Rates for Energy Program.

As amended by SB 699, Section 364 of the Public Utilities Code added the following additional requirements.

1. Requires the Commission to open a new proceeding or phase of an existing proceeding by July 1, 2015, to consider adopting standards or rules to address the physical security risks to the distribution systems of electrical corporations.
2. The standards or rules shall be prescriptive or performance based, or both.
3. The standards or rules may be based on risk management practices as appropriate, for each substantial type of distribution equipment or facility.
4. The standards or rules shall provide for high-quality, safe, and reliable service.
5. In setting the standards or rules, the Commission shall consider cost, local geography and weather, applicable codes, potential physical security risks, national electric industry practices, sound engineering judgment, and experience.
6. Provides that the Commission may, consistent with other provisions of law, withhold from the public information generated or obtained pursuant to this section that the Commission deems would pose a security threat to the public if disclosed.

Appendix A to this rulemaking provides the full text of SB 699 amending Public Utilities Code Section 364.

1.2. Applicable Safety Standards Prior to the Amendment of Section 364 of the Public Utilities Code

Section 364 of the Public Utilities Code requires the Commission to adopt standards for distribution facilities that provide for high quality, safe, and reliable service. Among other things, the Commission has adopted several

decisions, GOs, and rules to provide the utilities with standards and guidance to ensure an adequate level of safe and reliable service. Pursuant to GOs 95, 128, 131-D, 165, 166, 167 and 174, Commission staff is currently routinely involved in the verification of the condition and operation of existing physical security protections. Additionally, D.14-12-025 now requires all utilities to discuss safety and risk assessments in every rate case.

The Commission adopted GO 95 in Decision (D.) 34884, dated December 23, 1941, and has amended GO 95 many times since then. GO 95 contains rules for the design, construction, and maintenance of overhead power lines and communication lines located outside of buildings. GO 95 was last modified by D.15-01-005 on January 21, 2015.

The Commission adopted GO 128 in D.73195, dated October 17, 1967, and has amended GO 128 several times since then. GO 128 contains rules for the design, construction, and maintenance of underground electrical supply systems used in connection with public utility service and underground communication systems used in connection with public utility service located outside of buildings. GO 128 was last modified on January 13, 2005, in D.05-01-030.

The Commission adopted GO 131-D in D.94-06-014, dated June 8, 1994, which became effective July 8, 1994. GO 131-D requires that no electric public utility shall begin construction in this state of any new electric generating plant, or of the modification, alteration, or addition to an existing electric generating plant, or of electric transmission/power/distribution line facilities, or of new, upgraded or modified substations without first obtaining approval from the Commission. GO 131-D was last modified in D.95-08-038 on August 11, 1995, with the modifications effective on September 10, 1995.

On March 31, 1997, D.97-03-070 adopted GO 165. It was later revised by D.13-06-011 on June 27, 2013. Among other things, GO 165 established standards for inspection for transformers, switching/protective devices, regulators/capacitors, overhead conductor and cables, street lighting, and wood poles. GO 165 also set forth reporting responsibilities and called for the ability of Commission staff to inspect records of inspections consistent with Public Utilities Code Section 314(a).

On July 23, 1998, the Commission issued D.98-07-097 to establish GO 166, which set forth 11 standards for electric service reliability and safety during emergencies and disasters. These standards ensure that utilities are prepared for emergencies in order to minimize damage and inconvenience resulting from electric system failures and major outages. GO 166 contains detailed requirements for emergency planning and performance during emergencies, and requires an investigation following every major outage. On May 4, 2000, the Commission issued D.00-05-022 to add Standards 12 and 13 and to define a Major Event. It was last revised on May 15, 2014, by D.14-05-020.

On May 6, 2004, the Commission issued D.04-05-017, adopting GO 167, which set forth enforcement of maintenance and operation standards for electric generating facilities. GO 167 was most recently modified on November 6, 2008 by D.08-11-009. Section 10.4 of GO 167 sets forth various requirements for reporting safety related and property damage incidents. Section 11.0 notifies of the requirement to cooperate with Commission staff during audits, inspections or investigations.

On October 25, 2012, the Commission adopted D.12-10-029 to establish GO 174. The purpose of GO 174 is to set forth uniform requirements for substation inspections. Among other things, GO 174 requires the inspection of

perimeter fences and gates and sets forth record keeping and reporting responsibilities for all inspections performed.

In addition to already established standards and procedures listed above, SB 699 now requires the Commission to develop additional security measures. These additional security measures will help ensure an adequate level of safety for electrical supply facilities of electrical corporations. This rulemaking will be the procedure that the Commission uses to establish the necessary additional security measures.

1.3. Discussion Pertaining to SB 699

Ensuring the physical security of electrical supply facilities is of great importance in order to provide high quality, safe, and reliable service. In order to protect the electrical supply facilities of electrical corporations from security threats, the Commission has decided to undertake rulemaking on this issue. This rulemaking will provide for the regulatory framework pertaining to the physical security risks to the electrical supply facilities of electric corporations and will be consistent with the requirements set forth in SB 699, which amended Section 364 of the Public Utilities Code.

The April 2013 attack on the Metcalf Substation, and subsequent new standards set out by NERC have emphasized the need for standards to ensure the physical security of the electric grid. In California, SB 699 amended Public Utilities Code Section 364 to require the Commission to address physical security risks at the electrical supply level via the development of new rules and standards. As a result of SB 699, Commission Staff drafted a whitepaper, which

was released February 2015.[7] In this paper, Commission staff provides various recommendations and opinions the Commission may consider during this rulemaking process.[8]

Among other things, SB 699 requires the Commission to consider local geography and weather, and applicable codes when setting its standards or rules. Furthermore, SB 699 allows the Commission to consider options that include the nondisclosure to the public of any sensitive information, that if disclosed could pose a security threat.

Considering the wide possibilities of potential attacks, various equipment designs, and potential costs of implementing procedures, and rules for the security of the electrical supply facilities within the various utilities, a "one size fits all" approach may not be feasible. This rulemaking will consider and solicit input from the utilities and other interested persons on what rules and procedures should be adopted by this Commission.

2. Events Leading to Assembly Bill (AB) 1650

In September 2011, there were widespread outages in the Pacific Southwest that adversely impacted drinking water supplies due to the lack of electricity at pumping stations. In December 2011, there was a severe wind

---

[7] The whitepaper, titled *Regulation of Physical Security for the Electric Distribution System*, February 2015 is attached as Appendix B and is also available at www.cpuc.ca.gov/NR/rdonlyres/930FCC00-BE2F-4BCF-9B68-2CA2CDC38186/0/PhysicalSecurityfortheUtilityIndustry20150210.pdf.

[8] As indicated in the whitepaper, the views presented in the whitepaper are those of the staff and do not necessarily represent the views of the five member California Public Utilities Commission. This paper is intended to initiate a dialog on the topics discussed and any recommendations are preliminary. Staff may revise this whitepaper based on further discussion and any comments received.

storm that caused major damage throughout the San Gabriel Valley, including the loss of power to thousands of utility customers for a significant period of time. Many utility customers and local governmental entities were not provided sufficient information from the utilities regarding the status of the power outage or other damages caused by the windstorm.

2.1. Section 768.6 of the Public Utilities Code

AB 1650 added Section 768.6 to the Public Utilities Code to require the Commission in an existing proceeding to establish standards for disaster and emergency preparedness plans for electrical corporations and any water company regulated by the Commission. This rulemaking is concerned with implementing the addition of Section 768.6 of the Public Utilities Code.

Section 768.6 requires the following:

1. The Commission shall establish standards for disaster and emergency preparedness plans within an existing proceeding, including, but not limited to, the use of weather reports to preposition manpower and equipment before anticipated severe weather, methods of improving communications between governmental agencies and the public, and methods of working to control and mitigate an emergency or disaster and its aftereffects. The Commission, when establishing standards pursuant to this subdivision, may make requirements for small water corporations similar to those imposed on class A water corporations.
2. An electrical corporation shall develop, adopt, and update an emergency and disaster preparedness plan in compliance with the standards established by the Commission.
3. In developing and adopting an emergency and disaster preparedness plan, an electrical corporation shall invite appropriate representatives of every city, county, or city and county within that electrical corporation's service area to meet with, and provide consultation to, the electrical corporation.

4. Every city, county, or city and county within the electrical corporation's service area may designate a point of contact for the electrical corporation to consult with on emergency and disaster preparedness plans. The point of contact shall be provided with an opportunity to comment on draft emergency and disaster preparedness plans.

5. For the purposes of best preparing an electrical corporation for future emergencies or disasters, an emergency and disaster preparedness plan shall address recent emergencies and disasters associated with the electrical corporation or similarly situated corporations, and shall address remedial actions for possible emergencies or disasters that may involve that corporation's provision of service.

6. Every two years, in order to update and improve that electrical corporation's emergency and disaster preparedness plan, an electrical corporation shall invite appropriate representatives of every city, county, or city and county within that electrical corporation's service area to meet with, and provide consultation to, the electrical corporation.

7. For the purposes of best preparing an electrical corporation for future emergencies or disasters, an electrical corporation updating its emergency and disaster preparedness plan shall review the disasters and emergencies that have affected similarly situated corporations since the adoption of the plan, remedial actions taken during those emergencies or disasters, and proposed changes to the plan. The electrical corporation shall adopt in its plan the changes that will best ensure the electrical corporation is reasonably prepared to deal with a disaster or emergency.

8. Any meeting between the electrical corporation and every city and county within the electrical corporation’s service area shall be noticed and shall be conducted in a public meeting that allows for the participation of appropriate representatives of counties and cities within the electrical corporation's service area. A county participating in a meeting may inform each city within the county of the time and place of the meeting. An electrical corporation holding a meeting shall provide

participating counties and cities with the opportunity to provide written and verbal input regarding the corporation's emergency and disaster preparedness plan. For purposes of this public meeting, an electrical corporation may convene a closed meeting with representatives from every city, county, or city and county within that electrical corporation's service area to discuss sensitive security-related information in the electrical corporation's emergency and disaster preparedness plan and to solicit comment. An electrical corporation shall notify the Commission of the date, time, and location of the meeting. An electrical corporation shall conduct initial meetings no later than April 1, 2013, and shall conduct meetings every two years thereafter. An electrical corporation shall memorialize these meetings and shall submit its records of the meetings to the Commission.

9. A water company regulated by the Commission shall develop, adopt, and update an emergency and disaster preparedness plan in compliance with the standards established by the Commission. This requirement shall be deemed fulfilled when the water company files an emergency and disaster preparedness plan pursuant to another state statutory requirement. A water company developing, adopting, or updating an emergency and disaster preparedness plan shall hold meetings with representatives from each city, county, or city and county in the water company's service area regarding the emergency and disaster preparedness plan. An electrical corporation or a water corporation may fulfill a meeting requirement imposed by this section by making a presentation regarding its emergency and disaster preparedness plan at a regularly scheduled public meeting of each disaster council created pursuant to Article 10 (commencing with Section 8610) of Chapter 7 of Division 1 of Title 2 of the Government Code within the corporation's service area, or at a regularly scheduled public meeting of the governing body of each city, county, or city and county within the service area.

Appendix C to this rulemaking provides the full text of AB 1650 creating Public Utilities Code Section 768.6.

2.2. Emergency and Disaster Preparedness Plans for Electrical Corporations and Regulated Water Corporations Prior to the Addition of Public Utilities Code Section 768.6

Ensuring that electrical corporations and regulated water companies are adequately prepared during an emergency is of great importance. Over many years, the Commission has implemented disaster preparedness measures by adopting decisions, industrial standards, GOs, and rules to provide the utilities with standards and guidance regarding disaster preparedness.

As noted above, the Commission issued D.98-07-097 to establish GO 166. GO 166, among other things, requires electric utilities to annually file updated emergency response plans, including requiring the utility to notify local governments of its annual emergency response exercise. Additionally, GO 166 requires training and planning for deployment of personnel in anticipation of an event that may result in a major outage. However, it does not currently require deployment of personnel in the event of anticipated severe weather.

GO 103-A became effective on September 10, 2009, with the adoption of Resolution No. W-4823. GO 103-A sets forth various minimum standards for operation, maintenance, design and construction in regard to regulated water companies. Among other things, GO 103-A requires regulated water companies to cooperate with the Commission to "promote a reduction in hazards within the industry and to the public and requires the report of accidents that may disrupt the supply of water or impact continuity of service."

In order to ensure that electrical corporations and regulated water companies are sufficiently prepared for an emergency or other disaster, the Commission has undertaken various actions to provide guidance in preparing for a disaster or emergency. GOs 166 and 103-A provide utilities with basic

guidance in preparing for emergencies and other disasters, but does not provide all of the requirements set forth in AB 1650. AB 1650 helps to provide additional guidance in preparing for natural disasters and other emergencies. AB 1650 requires that the Commission undertake rulemaking to provide further guidance and sets forth various requirements that electrical corporations and regulated water companies must comply with to ensure that these utilities are adequately prepared for an emergency or other disasters.

2.3. Discussion Pertaining to AB 1650

Ensuring that utilities are adequately prepared for emergencies and other disasters is of great importance in order to provide high quality, safe, and reliable service. In order to ensure that regulated utilities are sufficiently prepared to deal with emergencies and other disasters, the Commission is opening this rulemaking to provide for the regulatory framework concerning emergency and disaster preparedness plans that regulated utilities shall adopt in order to be better prepared for disasters and other emergencies.

With input from the public and local agencies, the Commission will ensure electric corporations and regulated water companies have emergency preparedness plans that will be better able to help protect the public from disruption in electricity and water supply during emergencies or other disasters and consistent with the requirements of Section 768.6 to the Public Utilities Code. Part of this rulemaking is to solicit input from the utilities and other interested persons on what rules and procedures should be adopted by this Commission.

3. Preliminary Scope

As required by the Commission's Rules of Practice and Procedure Rule 7.1(d), this order initiating the rulemaking includes a preliminary scoping memo as set forth below.[9] The purpose of this rulemaking is to establish new rules and standards and to update existing requirements regarding the physical security of electrical supply facilities, in a manner which is consistent with SB 699 and to ensure that electrical corporations and regulated water companies have adequate disaster and emergency preparedness plans in effect that are consistent with AB 1650.

3.1. Issues to be Considered Pursuant to SB 699

The issues to be considered in this proceeding related to SB 699 may include, but are not limited to the following:

1. What are the key potential physical security risks to electrical supply facilities?
2. What new rules, standards, or General Orders or modifications to existing policies should the Commission consider to mitigate physical security risks to electrical supply facilities?
3. Should any new rules, standards, or General Orders or modifications to existing policies apply to all electrical supply facilities within the jurisdiction of the Commission, including facilities owned by publicly owned electrical utilities and rural electric cooperatives?
4. Are there other factors not listed in Section 364(b) of the Public Utilities Code that the Commission should consider when adopting any new rules, standards, or General

[9] All references to Rules are to the Commission's Rules of Practice and Procedure.

Orders or modifications to existing policies during this rulemaking?

5. What new rules or standards or modifications to existing policies should the Commission consider to allow for adequate disclosure of information to the public without disclosing sensitive information that could pose a security risk or threat if disclosed?

6. What is the role of cost and risk management in relation to the mitigation of any potential security risks to electrical supply facilities?

7. Should any new rules, standards, or General Orders or modifications to existing policies the Commission considers be prescriptive or performance based, or both?

8. What new rules, standards, or General Orders or modifications to existing policies should the Commission consider to ensure continued operation, reliability and safety during periods of emergencies and disasters as it relates to security of electrical supply facilities?

3.2. Issues to be Considered Pursuant to AB 1650

The issues to be considered in the subsequent phases of this proceeding under AB 1650 may include, but are not limited to the following:

1. What elements should be included in the electrical corporations' and regulated water companies' emergency and disaster preparedness plans?

2. What new rules, standards, or General Orders or modifications to existing policies should the Commission consider to ensure that electrical corporations and regulated water companies are in compliance with the statutory requirements of Public Utilities Code Section 768.6?

3. Should any new rules, standards, or General Orders or modifications to existing policies apply to all electrical supply facilities within the jurisdiction of the Commission,

including facilities owned by publicly owned electrical utilities and rural electric cooperatives?

4. Should the requirements for small water corporations be similar to those imposed on Class A water companies?
5. Should any new rules, standards, or General Orders, or modifications to existing policies be adopted to ensure that counties and cities have an opportunity to participate in the preparation of emergency and disaster preparedness plans?

4. Preliminary Schedule and Initial Comments

Public Utilities Code Section 1701.5(a) provides that in a quasi-legislative proceeding, the Commission shall resolve the issues raised in the scoping memo within 18 months of the date the scoping memo is issued. However, Section 1701.5(b) provides that the assigned Commissioner may specify in the scoping memo a resolution date of more than 18 months if the scoping memo includes specific reasons for the necessity of a later date.

Due to the complexity of this rulemaking, the number of respondents involved, the number of diverse issues presented, and the potential need for multiple phases, this matter will not be able to be concluded within 18 months. Therefore, it is preliminarily determined pursuant to Section 1701.5(b) that Phase I of this proceeding should be resolved within 24 months.

As noted above, this Order Instituting Rulemaking (OIR) will be conducted in phases. Phase I will pertain to the requirements imposed on electrical corporations by SB 699. Additional phases of this order instituting rulemaking will pertain to the requirements imposed on electrical corporations and regulated water companies pursuant to AB 1650.

The preliminary schedule for this proceeding is stated below in Table 1:

Table 1

30 days from Issuance of this OIR	Are the Questions set forth above in the Preliminary Scope the Appropriate Questions to Consider? Should the Commission Consider Additional Questions? Are there Other Issues in this Proceeding that the Commission Should Consider?
TBD	Prehearing Conference on Phase I issues
TBD	Scoping Memo on Phase I issues, and on final category and hearing determinations
TBD	Workshop(s) as needed on Phase I issues
TBD	Comments on Issues Presented at Workshop(s)
TBD	Reply to Comments from Workshop(s)
24 Months from Issuance of Scoping Memo	Proposed Decision on Phase I issues

A complete schedule for later phases of this proceeding will be set by later rulings of the assigned Commissioner or Administrative Law Judge.

5. Proceeding Category and Need for Hearing

Rule 7.1(d) specifies that an OIR will preliminarily determine the category of the proceeding and the need for hearing. As a preliminary matter, we determine that this proceeding is quasi-legislative as defined in Rule 1.3(d). It appears that the issues may be resolved through comments and workshops without the need for evidentiary hearings. In the event that an evidentiary hearing becomes necessary, the assigned Commissioner or Administrative Law Judge will issue a ruling that sets forth the process that will be used, and the schedule to be followed.

Any person who objects to the preliminary categorization of this rulemaking as quasi-legislative or to the preliminary hearing determination shall state any objections and material facts they believe require a hearing in their responses to the questions herein. After considering any comments on the preliminary categorization or preliminary hearing determination, the assigned Commissioner will issue a scoping ruling making a final category and hearing determination; this final determination as to categorization is subject to appeal as specified in Rule 7.6(a).

6. Respondents

The following are respondents in Phase I of this OIR: Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), San Diego Gas and Electric Company (SDG&E), PacifiCorp, CALPECO (Liberty Utilities) and Bear Valley Electric Service. Phase II of this OIR includes the above named respondents and also includes all Class A, B, C and D water companies regulated by the Commission.

7. Service of OIR

This OIR shall be served by the Commission on all respondents. In the interest of broad notice, this OIR will also be served on the official service lists for the following proceedings:

> R.14-08-012 (Order Instituting Rulemaking to Consider Proposed Amendments to General Order 95);
>
> R.01-10-001 (Order Instituting Rulemaking to Revise Commission General Order Numbers 95 & 128);
>
> R.08-11-005 (Order Instituting Rulemaking to Revise and Clarify Commission Regulations Relating to Safety of Electric Utility and Communications Infrastructure Provider Facilities);

R.02-11-039 (Rulemaking to Implement the Provisions of Public Utilities Code Section 761.3 Enacted by Chapter 19 of the 2001-2002 Second Extraordinary Legislative Session);

R.10-09-001 (Order Instituting Rulemaking to Implement Commission Regulations Relating to the Safety of Electric Utility Substations);

R.07-12-015 (Order Instituting Rulemaking on the Commission's Own Motion to Revise General Order 103);

This OIR will also be served on all California Publicly Owned Electric Utility Companies listed in Appendix D;

This OIR will also be served on all Rural Electric Cooperatives listed in Appendix E;

This OIR will also be served on the Public Owned Utilities Representatives and Agents listed in Appendix F;

This OIR will also be served on Facilities-Based Communications Carriers authorized to operate in California listed in Appendix G;

This OIR will also be served on the service list for Resolution No. W-4823 (Order Authorizing Revisions To General Order 103-A Section II.3.C.5, Minimum Standards For Repairs, And Section IV.1.A Method Of Measuring Service) listed in Appendix H; and.

Respondents Pacific Gas and Electric (PG&E), Southern California Edison (SCE), San Diego Gas and Electric (SDG&E), PacifiCorp, CALPECO (Liberty Utilities) and Bear Valley Electric Service are directed to serve a copy of this OIR on every city, county, or city and county within its service area in California. Service of this OIR on every city, county or city and county by the Respondents should be done as soon as feasibly possible, but no later than 30 days after this OIR is served upon the Respondents by the Commission. Within 45 days of

service of this OIR, Respondents shall file proof of service on every city, county or city and county with the Commission.

Service of this OIR does not confer party status or place a person who has received such service on the Official Service List for this proceeding.

8. Filing and Service of Comments and Other Documents

Filing and service of comments and other documents in the proceeding are governed by the rules contained in Article 1 of the Commission's Rules of Practice and Procedure. (See particularly Rules 1.5 through 1.10 and 1.13.)

If you have questions about the Commission's filing and service procedures, contact the Docket Office (Docket_office@cpuc.ca.gov) or check the Practitioners' Page on our web site at www.CPUC.ca.gov.

9. Addition to Official Service List

Addition to the official service list is governed by Rule 1.9(f) of the Commission's Rules of Practice and Procedure.

Respondents are parties to the proceeding (see Rule 1.4(d)) and will be immediately placed on the official service list.

Any person will be added to the "Information Only" category of the official service list upon request, for electronic service of all documents in the proceeding, and should do so promptly in order to ensure timely service of comments and other documents and correspondence in the proceeding. (See Rule 1.9(f).) The request must be sent to the Process Office by e-mail (process_office@cpuc.ca.gov) or letter (Process Office, California Public Utilities Commission, 505 Van Ness Avenue, San Francisco, California 94102). Please include the Docket Number of this rulemaking in the request.

Persons who file responsive comments thereby become parties to the proceeding (see Rule 1.4(a)(2)) and will be added to the "Parties" category of the official service list upon such filing. *In order to assure service of comments and other documents and correspondence in advance of obtaining party status, persons should promptly request addition to the "Information Only" category as described above;* they will be removed from that category upon obtaining party status.

10. Subscription Service

Persons may monitor the proceeding by subscribing to receive electronic copies of documents in this proceeding that are published on the Commission's website. There is no need to be on the official service list in order to use the subscription service. Instructions for enrolling in the subscription service are available on the Commission's website at http://subscribecpuc.cpuc.ca.gov/.

11. Public Advisor

Any person or entity interested in participating in this Rulemaking who is unfamiliar with the Commission's procedures should contact the Commission's Public Advisor's Office in San Francisco at (415) 703-2074 or (866) 849-8390 or e-mail public.advisor@cpuc.ca.gov. The TTY number is (866) 836-7825.

12. Intervenor Compensation

Any party that expects to claim intervenor compensation for its participation in this rulemaking must file its notice of intent to claim intervenor compensation within 30 days of the filing of comments, except that notice may be filed within 30 days of a prehearing conference in the event that one is held. (See Rule 17.1(a)(2).)

13. *Ex Parte* Communications

This proceeding is subject to Article 8 of the Commission's Rules, which specifies the standards to be followed for communicating with a decision maker. Pursuant to Rule 8.3(a), *ex parte* communications are allowed without any restrictions or reporting requirements unless an appeal of the categorization pursuant to Rule 7.6 is successful or until the categorization of this proceeding, or the applicable phase of this proceeding, is changed from quasi-legislative

Therefore, **IT IS ORDERED** that:

1. Pursuant to Rule 6.1 of the Commission's Rules of Practice and Procedure, this rulemaking is instituted on the Commission's own motion to establish policies, procedures, and rules pertaining to the physical security for the electric supply systems of electrical corporations within California consistent with Public Utilities Code Section 364.

2. Pursuant to Rule 6.1 of the Commission's Rules of Practice and Procedure, this rulemaking is instituted on the Commission's own motion to establish standards for disaster and emergency preparedness plans for electrical corporations and regulated water companies in California consistent with Public Utilities Code Section 768.6.

3. This rulemaking will be conducted in phases. Phase I will pertain to the physical security for the electric supply systems of electrical corporations and additional phases will pertain to disaster and emergency preparedness plans for electrical corporations and regulated water companies.

4. This rulemaking may consider whether any new rules, standards, or General Orders or modifications to existing policies should apply to all electrical supply facilities within the jurisdiction of the Commission, including facilities owned by publicly owned utilities and rural electric cooperatives.

5. Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), San Diego Gas and Electric Company (SDG&E), PacifiCorp, CALPECO (Liberty Utilities), and Bear Valley Electric Service are named as respondents to both phases of this proceeding. All regulated Class A, B, C and D water companies listed in official Commission records are named respondents in Phase II of this proceeding.

6. This proceeding is preliminarily classified as quasi-legislative, and it is preliminarily determined that evidentiary hearings will not be necessary.

7. No later than 30 days after the Commission adopts this Order Instituting Rulemaking, any person may file opening comments addressing whether the questions set forth above in sections 3.1 and 3.2 are the appropriate questions to consider; whether the Commission should consider additional questions; and whether there are other issues in this proceeding that the Commission should consider.

8. Any person may file comments on the scope, schedule, categorization, or need for hearing no later than 30 days after the Commission adopts this Order Instituting Rulemaking.

9. The Executive Director shall cause this Order Instituting Rulemaking (OIR) to be served on the following Respondents: Pacific Gas and Electric Company (PG&E), Southern California Edison Company (SCE), San Diego Gas and Electric Company (SDG&E), PacifiCorp, CALPECO (Liberty Utilities); Bear Valley Electric Service; and all regulated Class A, B, C and D water companies. In the interest of broad notice, this OIR shall also be served on the official service lists in Rulemaking (R.) 14-08-012; R.01-10-001; R.08-11-005; R.02-11-039; R.10-09-001; R.07-12-015; all Publicly-Owned Electric Companies, rural electric cooperatives and other Publicly-Owned Utilities' Representatives listed in Appendices D, E,

and F; on Facilities-Based Communications Carriers authorized to operate in California listed in Appendix G; and the service list from Resolution No. W-4823 listed in Appendix H.

10. Respondents Pacific Gas and Electric Company, Southern California Edison Company, San Diego Gas and Electric Company, PacifiCorp, CALPECO (Liberty Utilities) and Bear Valley Electric Service are shall serve a copy of this Order Instituting Rulemaking (OIR) on every city, county, or city and county within its service area in California. Service of this OIR on every city, county or city and county by the Respondents shall be done no later than 30 days after this OIR is served upon the Respondents by the Commission. Within 45 days of service of this OIR, Respondents shall file proof of service on every city, county or city and county with the Commission.

11. A party that expects to request intervenor compensation for its participation in this rulemaking must file its notice of intent to claim intervenor compensation within 30 days of the filing of comments, except that notice may be filed within 30 days of a prehearing conference in the event that one is held (see Rule 17.1(a)(2).).

12. *Ex parte* communications in this Rulemaking are governed by Rule 8.3(a) of the Commission's Rules of Practice and Procedure.

13. The assigned Commissioner or Administrative Law Judge may adjust the schedule identified herein and refine the scope of this proceeding as needed to promote the efficient and fair resolution of the rulemaking.

This order is effective today.

Dated _____, at San Francisco, California.

Appendix A

(Senate Bill 699 amending Public Utilities Code Section 364)

BILL NUMBER: SB 699 CHAPTERED

An act to amend Section 364 of the Public Utilities Code, relating to public utilities.

SB 699, Hill. Public Utilities: electric corporations.

Under existing law, the Public Utilities Commission has regulatory authority over public utilities, including electrical corporations, as defined. Existing law requires the commission to adopt inspection, maintenance, repair, and replacement standards for the distribution systems of electrical corporations in order to provide high-quality, safe, and reliable service. Existing law requires the commission to conduct a review to determine whether the standards have been met and to perform the review after every major outage.

This bill would require the commission, in a new proceeding, or new phase of an existing proceeding, to commence on or before July 1, 2015, to consider adopting rules to address physical security risks to the distribution systems of electrical corporations.

Under existing law, a violation of the Public Utilities Act or any order, decision, rule, direction, demand, or requirement of the commission is a crime.

Because the provisions of this bill are within the act and require action by the commission to implement its requirements, a violation of these provisions would impose a state-mandated local program by expanding the definition of a crime.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1.

The Legislature finds and declares all of the following:

(a) Physical threats to the electrical distribution system present risks to public health and safety and could disrupt economic activity in California.

(b) Ensuring appropriate actions are taken to protect and secure vulnerable electrical distribution system assets from physical threats that could disrupt safe and reliable electric service, or disrupt essential public services, including safe drinking water supplies, are in the public interest.

(c) Proper planning, in 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 the potential consequences of such attacks.

SEC. 2.

Section 364 of the Public Utilities Code is amended to read:

364.

(a) The commission shall adopt inspection, maintenance, repair, and replacement standards, and shall, in a new proceeding, or new phase of an existing proceeding, to commence on or before July 1, 2015, consider adopting rules to address the physical security risks to the distribution systems of electrical corporations. The standards or rules, which shall be prescriptive or performance based, or both, and may be based on risk management, as appropriate, for each substantial type of distribution equipment or facility, shall provide for high-quality, safe, and reliable service.

(b) In setting its standards or rules, the commission shall consider: cost, local geography and weather, applicable codes, potential physical security risks, national electric industry practices, sound engineering judgment, and experience. The commission shall also adopt standards for operation, reliability, and safety during periods of emergency and disaster. The commission shall require each electrical corporation to report annually on its compliance with the standards or rules. Except as provided in subdivision (d), that report shall be made available to the public.

(c) The commission shall conduct a review to determine whether the standards or rules prescribed in this section have been met. If the commission finds that the standards or rules have not been met, the commission may order appropriate sanctions, including penalties in the form of rate reductions or monetary fines. The review shall be performed after every major outage. Any money collected pursuant to this subdivision shall be used to offset funding for the California Alternative Rates for Energy Program.

(d) The commission may, consistent with other provisions of law, withhold from the public information generated or obtained pursuant to this section that it deems would pose a security threat to the public if disclosed.

SEC. 3.

No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution. *(End of Appendix A)*

Appendix B

(*Regulation of Physical Security for the Electric Distribution System*, February 2015)

Regulation of Physical Security for the Electric Distribution System

February 2015

Ben Brinkman
Safety and Enforcement Division, Electric Safety and Reliability Branch

Connie Chen
Energy Division, Infrastructure Planning and Permitting Branch

Arthur O'Donnell
Energy Division, Infrastructure Planning and Permitting Branch

Chris Parkes
Safety and Enforcement Division, Risk Assessment Section

Edmund G. Brown Jr., *Governor*

The views presented in this paper are those of staff and do not necessarily represent the views of the five member California Public Utilities Commission. This paper is intended to initiate a dialog on the topics discussed and any recommendations are preliminary. Staff may revise this paper based on further discussion and comments received.

EXECUTIVE SUMMARY AND MAJOR TAKEAWAYS

Executive Summary

On April 16, 2013, Pacific Gas and Electric Company's (PG&E's) Metcalf Substation sustained millions of dollars in damages from a gunshot attack that destroyed several transformer oil tanks at the facility. Fortunately, no customers lost power due to the event, but a similar attack under different circumstances might have been catastrophic.

As a result of this attack, public concern regarding security of the electric grid, which is typically reserved for cyber protection of electric facilities, expanded to include concern over physical security measures for the electric grid. The Federal Energy Regulatory Commission (FERC) tasked the North American Electric Reliability Corporation (NERC) with developing a standard for physical security at the most critical bulk-power level substations. While these new federal standards are limited to a select group of transmission level substations, the California Public Utilities Commission (CPUC or the Commission) is examining grid security at all levels of the electric supply system, including the distribution level, and is re-evaluating its existing policies and oversight activities for electric system security.

CPUC staff held a two day workshop on substation physical security in June, 2014. CPUC staff assembled a panel of electric grid security experts to discuss major issues in physical security. The first day consisted of public workshops, during which PG&E elaborated on its security improvements since the Metcalf substation attack, and the expert panel discussed current security threats and best practices in physical security. During the second day, representatives from the major California utilities presented their specific physical security measures to CPUC staff in a closed door meeting, followed by a roundtable discussion of existing and pending state and federal security related legislation and regulations.

On September 25, 2014, California's governor signed into law California Senate Bill 699 (See Appendix A) which requires the Commission to develop rules for physical security of the electric distribution system.

The purpose of this whitepaper is to discuss the current and potential regulatory framework around electric distribution system physical security, to present the process involved in evaluating potential security measures, to identify questions the Commission should address in developing rules for physical security, and to recommend a possible methodology for utility electric distribution system physical security planning.

Major Takeaways

1. Security of the electric distribution system is an important concern for protection of life and to provide and maintain a safe and reliable power delivery system. Physical security measures represent important considerations in an asset protection scheme that includes cybersecurity and information security. It is impossible to completely separate physical security from cyber and information security.

2. Although physical attacks on electric facilities occur with some regularity, none to date have caused major, widespread outages affecting the stability of the grid. However, given recent events and analysis, and the potential for malevolent actors to disrupt the electrical system, physical security for the electric grid is a significant concern.

3. In 2014, NERC developed a new standard for electric grid physical security, however NERC CIP[1] security regulations are limited to bulk-power assets[2] and therefore do not apply to the lower voltage electric distribution system.

4. Because of the limits of federal regulations, a critical role exists for state government, including the Commission, in enforcing physical security at the distribution level. In fact, existing Commission rules already establish some requirements regarding distribution system physical security.

5. New state legislation[3] mandates Commission action to develop rules for physical security for the distribution system in a new or existing proceeding.

---

[1] Critical Infrastructure Protection.
[2] Bulk power here refers to those transmission and generation assets covered by NERC standards. The definition of the "bulk-power" system has been evolving through a stakeholder process but typically generally refers to assets operating at a voltage over 100kV.
http://www.mondaq.com/unitedstates/x/215222/Oil+Gas+Electricity/FERC+Approves+Revised+Bulk+Electric+System+Definition+And+Reserves+Authority+To+Determine+Local+Distribution+Facilities

6. The recent state legislation addresses only the "distribution system." However, the processes and elements of physical security planning are applicable to all levels of the electric supply grid.

7. Security planning should consider multiple factors. Public Utilities Code Section 364, as amended by Senate Bill 699, enumerates cost, local geography and weather, applicable codes, potential physical security risks, national electric industry practices, sound engineering judgment, and experience. Other impacts including environmental impact should also be considered.

8. Although the specific methodologies and threats differ, varied industries, including electric utilities, choose from a similar menu of options for physical security mitigation. Physical security includes practices to deter, detect, and respond to unauthorized access or attacks. This includes actions such as constructing walls, using intrusion detection and lighting, and employing security forces. Utilities augment these purely physical efforts with cyber and information security activities and security policies and practices.

9. Electric system physical security can be costly; therefore, given the vast array of distribution equipment, design, and other external considerations, it is virtually impossible for regulators to establish a "one-size-fits-all" approach that would work for all utilities. A performance based approach with reliable metrics lends itself well to a system with varied equipment. Detailed prescriptive measures will likely not be feasible in many instances; however general guidelines and requirements may be appropriate. In addition, the utilities should consider accepted good practices as developed by industry organizations.

10. A sound planning methodology would use a risk based approach. Under a risk based approach the Commission would require utility planners to identify and assess risks and vulnerabilities, develop mitigation plans from various alternatives, and assemble tests and metrics for evaluating their plans. The utility should consider alternatives and justify the alternatives chosen with respect to efficacy, cost, and other significant considerations.

---

[3] Senate Bill 699, amending Public Utilities Code Section 364.

11. The Commission should consider protection of critical security information as part of its regulatory standard development process. Because Senate Bill 699 specifies that the Commission may withhold from the public certain information whose release would pose a security threat, it would be appropriate for the rulemaking to consider the types of information that warrant confidential treatment under the statute.

Recommendations

1. The CPUC should open a rulemaking to evaluate and update existing requirements regarding physical security of the electric system, in a manner consistent with Senate Bill 699.

2. The CPUC should address the following during the rulemaking:

    - *What does the "distribution" system, as that term is used in Senate Bill 699, consist of?*
    - *Is there any jurisdictional overlap (FERC, NERC, CAISO, etc.)?*
    - *Should the CPUC rules include requirements for bulk-power level facilities?*
    - *Which sorts of rules are best – Prescriptive? Performance based? A combination?*
    - *How should risk be considered?*
    - *Should the Commission base its physical security rules on existing rules or standards, such as NERC CIP 14?*
    - *What constitutes "physical security" measures that should be adopted under Senate Bill 699?*
    - *At a high level, what elements are important in a physical security program?*
    - *How should the Commission balance cost with security?*
    - *How should the Commission balance environmental issues with security?*
    - *How should the Commission determine accepted best practices in physical security?*
    - *In enforcing the regulations on physical security, how should the Commission protect sensitive information? Are current confidentiality rules and practices sufficient?*

- *What metrics, tests, or drills can be employed to determine effectiveness of a security plan?*
- *What prescriptive guidelines should be included as part of the regulations?*
- *Should the rules apply to publicly owned utilities?*
- *How should the rules be enforced? What should be the timeline for the first security plan submissions and updates? What should be the implementation timeline?*
- *How often should the system be re-analyzed?*
- *What sorts of events should undergo root cause analysis?*
- *Should the Commission require the utilities to use independent security experts to prepare, vet or test the utility security plans*?
- *Should the Commission contract its own independent security expert to assist in development of rules*?

3. Commission rules should require a risk based approach to physical security planning. Under the recommended risk based approach, the utility would be required to identify and assess risks to its facilities and develop a plan to mitigate those risks. The utility would also be required to develop clear metrics to evaluate the success of its plan. The utility would present this plan to the Commission and submit updates to the plan as necessary. The utility would need to report annually on its compliance with the adopted rules, as required by Senate Bill 699.

4. The utility should be required to consider various alternatives and justify that the choices chosen are optimal with respect to mitigating risks at an appropriate cost level. The utilities should also consider additional factors, including those identified in Section 364 and also other factors, such as environmental impacts, when designing their security plans.

5. A hybrid approach, including the performance based rules referenced above along with some high level prescriptive guidelines, may be the optimal approach.

6. The utilities should justify their security planning choices based on industry best practices. The utilities should refer to existing standards such as IEEE standards on

Substation Physical Security[4] or other recognized industry standards in justifying their plans. The utilities should also be required to develop and employ metrics and regularly evaluate the results of those metrics as justification for continuing or changing their plans.

7. Drills and testing of the security plans should be included in every utility security plan. The drills should include surprise inspections and simulated real life events that stress the security system. Periodic testing of alarms, access, and monitoring equipment is also critical. Where appropriate, the utility should perform root-cause analysis of any failures detected in the drills.

8. The Commission may consider whether to require the utilities to vet their plans through independent third party experts before submission, and whether the utilities should use third parties in testing their plans. Additionally, the Commission should determine if it wishes to contract its own third party expert for assistance in development of rules.

9. Protection of sensitive information is a critical concern. The Commission should consider the appropriate confidentiality measures for sensitive security information. It may be appropriate for Commission staff to take appropriate training on protecting critical infrastructure information.

[4] IEEE Standards Association. 2014. See http://standards.ieee.org/findstds/standard/1402-2000.html

Contents

EXECUTIVE SUMMARY AND MAJOR TAKEAWAYS iii
Executive Summary iii
Major Takeaways iv
Recommendations vi
1.0. Introduction 1
2.0. Definition of Physical Security 2
2.1. Physical Security, Cybersecurity, and Information Security 4
3.0. Significant Incidents at Electrical Facilities 4
4.0. Federal and State Initiatives, Laws, and Regulatory Responses 7
4.1. Critical Infrastructure Protection Standards – CIPs 9
4.2. Other Physical Security Standards 12
4.3. Existing CPUC Regulation and Oversight Activities 12
4.3.1. Metcalf Attack and Metcalf Burglary 13
4.4 Physical Security Activities in other States and Power Agencies 14
5.0. Examples of Physical Security from Other Industries 15
5.1. Physical Security in the Nuclear Industry 15
5.2. Physical Security in the Chemical Industry 16
5.3. Physical Security for the Financial Sector 16
5.4. Military Physical Security 17
6.0. Risk Based Physical Security for the Electric Grid 17
6.1. Risk Management Process 17
6.2. Risk Identification and Assessment (Evaluate Risks, Threats, and Vulnerabilities) 18
6.3. Risk Mitigation (Control Risks) 20
6.3.1. Physical Mitigation 20
6.3.2. Policies and Procedures Related to Physical Security 25
6.3.3. Other Considerations for Risk Mitigation Planning 25
6.4. Metrics (Review Controls) 29
6.4.1. Prescriptive versus Performance Based Regulations 29

6.4.2. Control Metrics for Utility Distribution Systems 30
7.0. Proposed Next Steps for the Commission 32
7.1. Development of Rules Required by Senate Bill 699 32
7.1.1. Potential Model for Rules for Physical Security 32
7.1.2. Protection of Sensitive Information 37
8.0 Conclusion 38
Appendix A 40
Appendix B 42

1.0. Introduction

Recent events, in particular the April 2013 attack on the Metcalf Substation, and subsequent new standards by the North American Electric Reliability Corporation (NERC, formerly the North American Electric Reliability Council) have focused attention on the physical security of the electric grid. In California, new legislation at the state level requires the California Public Utilities Commission (CPUC) to develop rules to address physical security risks at the electric distribution level.

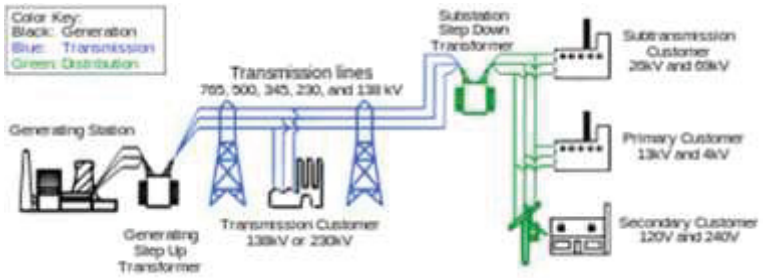
This whitepaper discusses the relevant issues in physical security for the electric distribution system, with a particular focus on advising policymakers on implementation scenarios for the new requirements codified in Section 364 of the Public Utilities Code, as amended by Senate Bill 699.[5] Section 364 of the Public Utilities Code requires, in part,

> *The commission… shall, in a new proceeding, or new phase of an existing proceeding, to commence on or before July 1, 2015, consider adopting rules to address the physical security risks to the distribution systems of electrical corporations. The standards or rules, which shall be prescriptive or performance based, or both, and may be based on risk management, as appropriate, for each substantial type of distribution equipment or facility, shall provide for high-quality, safe, and reliable service.*

The electric grid consists of generation, transmission, and distribution facilities. The transmission and distribution systems consist of overhead and underground lines, and substations which convert voltage levels and switch power. Generators typically deliver power to the bulk-power high voltage transmission system, which in turn delivers that power to the lower voltage distribution system for delivery to end users.[6] The bulk-power transmission system is generally defined as those lines and substations operating above 100 kV. Lower voltage level transmission lines and substations, often referred to as sub-transmission, operate from around 25 kV to 100 kV. Substations then convert these transmission and sub-transmission level voltages to lower distribution level voltages (typically 4 kV, 12 kV, or 15 kV) for delivery to end users.

[5] California State Senate Bill 699. See http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB699

[6] Also, increasing numbers of distributed energy resources and energy storage facilities interconnect at the distribution level.



Electric Delivery System[7]

Since the 2013 Metcalf Substation attack, and even before that attack, a great deal of public attention has focused on security at the bulk-power level. This whitepaper does not focus strictly on those assets, but discusses physical security measures in general for the entire electric grid. Most security measures pertinent to distribution substations also apply to transmission level substations, and elements of physical security pertinent to other distribution infrastructure also pertain to similar overhead and underground transmission facilities. The differences lie in the impact assessments and the particular structures involved in the physical security planning (e.g., poles verses towers).

2.0. Definition of Physical Security

Physical security, as opposed to cybersecurity, refers to physical deterrence, monitoring, and mitigation activities. A restrictive definition of physical security includes only those elements and strategies directly involved in physical protection- perimeter walls and fencing, lighting, cameras and security patrols. This paper adopts a somewhat more expansive definition, which also includes certain elements of policies, procedures and training related to the physical protection of grid facilities (e.g., background screening of guards) as well as some elements of cybersecurity necessary for the functioning of physical security safeguards (e.g., alarm interpretation software). This paper does not discuss in detail the security for critical bulk power transmission facilities covered under NERC regulations, but rather security for the entire electric delivery system including transmission and distribution facilities, including substations. The processes discussed here should apply to all types of utility facilities.

[7] Adapted by Congressional Research Service from: U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004, Figure 2.1.

The physical security of the bulk-power grid has long been a matter of concern for policy makers, and attention to these assets increased significantly following the 2013 Metcalf Substation attack. In June 2014 the Congressional Research Service prepared a paper entitled "Physical Security of the US Power Grid: High Voltage Transformer Substations." The paper focused on the threat to bulk-power level substations, and in particular the risks and vulnerabilities associated with transformers in these substations.

Even prior to the Metcalf attack, federal agencies conducted vulnerability studies of the electric grid. In 2011 NERC conducted Grid-Ex I. In this exercise, NERC determined that although the utilities "took appropriate steps to protect the grid," NERC should facilitate the development of updated physical security standards.[8] In 2013, following the Metcalf attack, NERC conducted Grid-Ex II, in which it determined that:

> *While the electricity industry has experienced occasional acts of sabotage or vandalism, a well-coordinated physical attack also presents particular challenges for how the industry restores power.... The extreme challenges posed by the Severe Event scenario provided an opportunity for participants to discuss how the electricity industry's mutual aid arrangements and inventories of critical spare equipment may need to be enhanced.*[9]

In 2013 FERC conducted its "Electrically Significant Locations" study in which it modeled power flow in the transmission system and identified 30 critical substations across the United States. Although disputed by some experts, the study also determined that disabling only 9 of these substations could potentially cause an extended national blackout.[10]

Although high voltage transmission level transformers are certainly a critical point of concern, they are not the only vulnerability in the electric grid. As such, on June 17 and 18, 2014, the CPUC held public and closed workshops on substation and overall grid physical security, which included participation by major utilities in the state as well as industry experts from NERC, Lawrence Livermore Laboratory, and the Department of Homeland Security (DHS). As part of planning this

---

[8] North American Electric Reliability Corporation (NERC), *2011 NERC Grid Security Exercise: After Action Report*, March 2012, p. ii.
[9] North American Electric Reliability Corporation (NERC), *Grid Security Exercise (GridEx II): After-Action Report*, March 2014, p.5.
[10] Rebecca Smith, "U.S. Risks National Blackout from Small-Scale Attack on Substations," *Wall Street Journal*, March13, 2014.

event, Commission staff also spoke with personnel from the Federal Bureau of Investigation (FBI). Much of the information in this paper was derived from information presented publicly by utility, industry and security experts at the event.

2.1. Physical Security, Cybersecurity, and Information Security

It is impossible to completely separate effective physical security measures from cyber security and information security measures.[11] A significant element of physical security involves alarms and visual monitoring (cameras). For these to be effective, information must be transmitted to control or security centers. Therefore, communications systems must remain intact and fully operational, making cyber protection a critical concern. Additionally, physical security measures can be rendered ineffective if critical information about those measures is made public.

3.0. Significant Incidents at Electrical Facilities

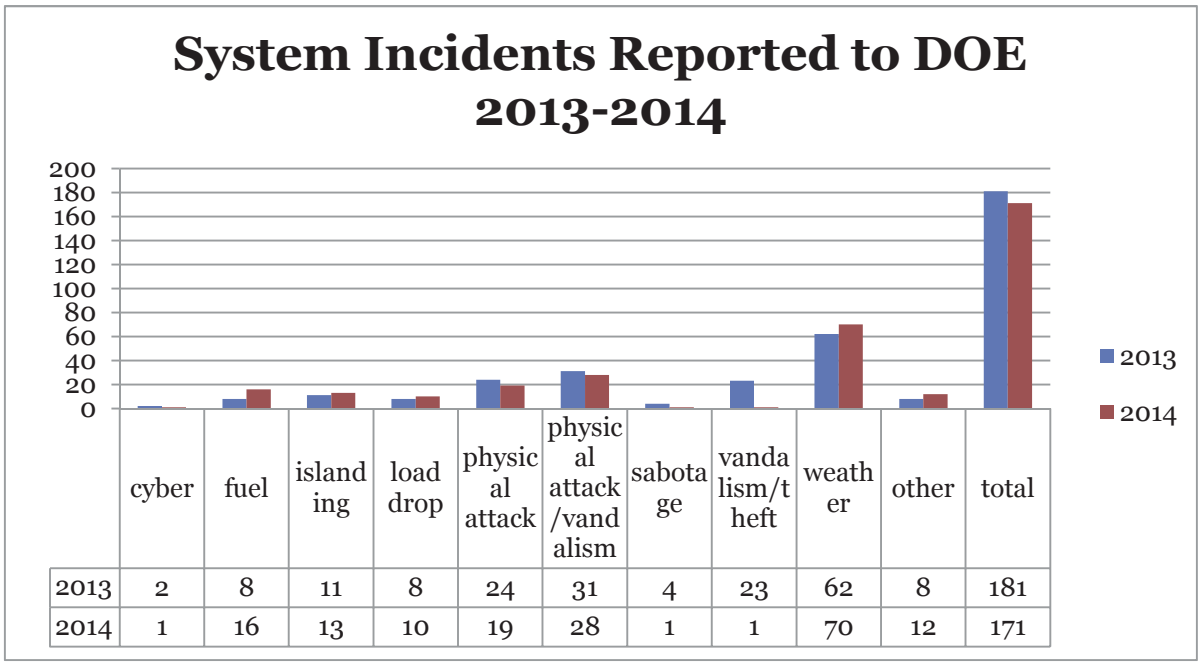
The major risks associated with a physical attack against electricity grid facilities are incidents that cause substantial enough damage, and result in widespread outages that last for days or weeks as critical equipment is repaired or replaced. While there have been many examples of extreme weather events – including heavy winds, tornadoes and hurricanes, ice storms, and fires beneath high voltage transmission lines -- that have resulted in such disruptions, to date in the United States there have been no such extended outages that stem from a planned attack on transmission or substation facilities.[12]

Even the damage to electric transformers at PG&E's Metcalf Substation did not cause outages, despite a cost of repairs estimated at $15.4 million. Some 100 bullets fired at the substation caused damage to 17 transformers and six circuit breakers, with the major damage being to transformer radiators that leaked 52,000 gallons of cooling oil. However, the incident did not result in any disruption of service.[13]

Still, vandalism and other physical attacks on utility facilities represent a substantial number of incidents reported to a federal agency. During 2013 and 2014 (reported through October 1), the

[11] CPUC Substation Security workshops, June 2014.
[12] Parformak, Paul W.; *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*, Congressional Research Service, June 17, 2014; pg. 2.
[13] SED Presentation to CPUC on PG&E Metcalf Incident and Substation Security, February 27, 2014.

U.S. Department of Energy's Office of Electricity Delivery and Energy Reliability received 352 incident reports; weather related events made up 37 percent while combined physical attacks/vandalism/sabotage were also declared in 37 percent. Cyber-attacks were responsible for just 3 of the reports, according to DOE. Fuel shortages, unintentional islanding and various electrical disturbances comprise the rest.



	cyber	fuel	islanding	load drop	physical attack	physical attack /vandalism	sabotage	vandalism/theft	weather	other	total
2013	2	8	11	8	24	31	4	23	62	8	181
2014	1	16	13	10	19	28	1	1	70	12	171

Source: DOE Submissions of all Electric Emergency Incident and Disturbance Reports (OE-417), http://www.oe.netl.doe.gov/oe417.aspx

Despite many incident reports that cited Physical Attack /Vandalism/Suspicious Activity or Sabotage, only two resulted in documented power outages or loss of load for more than 2 hours.[14] In contrast, weather incidents severe enough to be reported invariably affected hundreds to hundreds of thousands of utility customers, sometimes for extended periods.

Purposeful attacks on electric utility facilities may be reported to DOE as "sabotage" or vandalism (often including theft of copper wire), but they are rarely revealed in the media, although a few incidents have become public. In October 2005, a rifle attack was reported at a Progress Energy substation in Florida, which resulted in a small explosion, a transformer oil leak, and local power

[14] DOE Office of Electricity Delivery and Energy Reliability, web site report November 25, 2014. *http://energy.gov/oe/services/energy-assurance/monitoring-reporting-analysis/electric-disturbance-events-oe-417*

outage.[15] More recently, in June 2014, a device described as a "homemade bomb" by authorities ignited a small fire at a Nogales, AZ, substation. The fire left burn marks on a 50,000-gallon diesel storage tank at the Valencia substation without interrupting power to the area. The incident has been termed "sabotage" by DOE.

These incidents remain unsolved, but there has been one high-profile case in which federal investigators have identified and arrested a "lone wolf" perpetrator who caused several millions of dollars in damage to utility infrastructure.

In October 2013, the United States Department of Justice charged an Arkansas man with sabotage, a terrorist attack against a railroad and destruction of an energy facility, stemming from incidents that occurred over the course of several months in Lonoke County, AR. In one attack on August 21, 2013, the man allegedly removed over 100 bolts securing a 100 foot 500 kV transmission tower leaving only five in place, and proceeded to sever a shackle on a support wire. Subsequently, the tower fell onto nearby railroad tracks and was struck by a train, causing a brief power outage.

In a separate incident, on September 29, 2013, the same person allegedly set fire to an Entergy high voltage switching station, leaving behind a message: "You should have expected U.S."[16] Finally, on October 6, 2013, First Electric Cooperative experienced a power outage affecting 9,200 customers. Utility and law enforcement investigations indicated that two power poles had been cut and pulled down by a stolen tractor.[17]

A joint investigation by the Federal Bureau of Investigation, the Joint Terrorism Task Force and a dozen other federal, state and local agencies quickly led to an arrest less than one week following the final incident. The man, Jason Woodring of Jacksonville, AR, was indicted on 8 federal counts, including a terrorist attack, destruction of an energy facility, and illegal possession of weapons and drugs. As of January 2015, he awaits trial.

In most cases, it may be difficult to ascertain when an attack on utility facilities is a planned event meant to cause service disruptions, or a crime of opportunity by vandals.

---

[15] Parformak, op cit, pg. 7.
[16] "Power Grid is Attacked in Arkansas," New York Times, October 8, 2013
[17] U.S. Department of Justice, U.S. Attorney for the Eastern District of Arkansas, news release, October 12, 2013

On the eve of the new millennium, in 1999, when utilities around the globe prepared for a potential disruption to their computer-driven operations due to the infamous Y2K programming glitch, the Western U.S. grid saw only one actual system outage that resulted from a fallen transmission tower in Oregon. According to the California Independent System Operator (CAISO), the tower was adjacent to an Indian reservation. Someone reportedly hopped a fence, cut a guide wire and removed bolts, allowing a strong wind to topple the tower.[18]

Even though the actual impacts of reported physical attacks on the electric grid have been minimal, there is no reason to downplay the potential threat that a well-planned and coordinated attack on the grid might pose. A previously confidential 2013 analysis from the Federal Energy Regulatory Commission (FERC), which was publicly revealed by a *Wall Street Journal* article, warned that a coordinated attack on as few as nine electric transmission substations in various combinations around the country could potentially cause cascading outages in each of the nation's three synchronized power networks. Although the analysis itself was a cause for concern, it appeared that the public release of the information brought far greater criticism in Washington, D.C., with FERC officials and lawmakers condemning the newspaper for undermining grid security – although the news article did not identify what facilities were deemed at risk in the "worst case" scenario.[19]

However, the combination of the Journal article and the PG&E Metcalf incident has heightened the issue of physical security to a place more equal to the concerns expressed about cybersecurity.

4.0. Federal and State Initiatives, Laws, and Regulatory Responses

Efforts by the U.S. Government to define and address the security of the electricity system have waxed and waned over the past two decades, with concerns about physical security most often taking a back seat to perceived cybersecurity vulnerabilities. In 1996, for example, President Clinton's Administration established the President's Commission on Critical Infrastructure Protection to make recommendations on policies related to the vulnerabilities and threats to the

[18] O'Donnell, Arthur, "Soul of the Grid" 2004, pg.124.
[19] E&E News, "FERC's confidential threat analysis triggers political reaction," March 14, 2014.

nation's critical infrastructure.[20] The report, dated October 1997, found "no immediate crisis threatening the nation's infrastructures" but did recommend immediate actions on the cybersecurity front.[21] The recommendations eventually led to a Presidential Decision Directive No. 63 (PDD-63) in 1998, which set a goal of securing the nation's critical infrastructure from both physical and cyber-attacks by the year 2003.

The effort was soon superseded in the post-9-11 period, with the establishment of the Office of Homeland Security (later made a Cabinet-level Department) and subsequent passage of both the Critical Infrastructures Protection Act of 2001[22] and the Homeland Security Act of 2002.[23] These laws provided a set of policy goals and a statutory definition of critical infrastructure:

> *It is the policy of the United States 1) that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States.*[24]
>
> *[T]he term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.*[25]

In the intervening years, there have been many refinements to the structure of DHS and the various councils and committees established to advise it and the President. These developments tended to shift the emphasis of national policy to concentrate on cybersecurity of the grid, while emphasizing physical security of other critical infrastructures.[26] In the wake of Hurricane Sandy's devastating impacts on Northeastern states, the term "resiliency" has been added as a goal of critical infrastructure policies embodied in the most recent changes to the National Infrastructure

---

[20] Executive Order 13010 Critical Infrastructure Protection, Federal Register Vol. 61, No. 138, July 17, 1996.
[21] *Critical Foundations: Protecting America's Infrastructures,* President's Commission on Critical Infrastructure Protection, October 1997.
[22] 42 US Code 5195C
[23] Public Law 107-296, Sec. 214
[24] 42 US Code 5195C Sec. (c) (1).
[25] Sec. (e)
[26] Moteff, John D., *Critical Infrastructures: Background, Policy and Implementation*, Congressional Research Service, February 21, 2014, provides a detailed review of these developments from 1996 to the present.

Protection Plan (NIPP).[27] Resiliency considerations are an important element of substation security planning and risk assessment. NIPP, overseen by DHS' Office of Infrastructure Protection, was updated as a result of Presidential Policy Directive-21 (PPD-21) in February 2013. According to DHS director of strategy and policy Bob Kolasky, "[G]rowing interdependencies across infrastructure systems, particularly reliance on information and communications technologies, have produced new vulnerabilities to physical and cyber threats. The new plan NIPP 2013, guides efforts across the critical infrastructure community to enhance security and resilience in conjunction with national preparedness policy."[28]

This emphasis on cybersecurity is largely mirrored by the plethora of federal legislation introduced, considered and occasionally chaptered into law, while physical security has received far less legislative attention.[29]

4.1. Critical Infrastructure Protection Standards – CIPs

In the national regulatory arena, the interplay between the FERC and NERC has largely provided the platform for both physical security and cybersecurity efforts in the electric utility industry. FERC is a federal agency, successor to the Federal Power Administration, which has primary regulatory authority over interstate electric and natural gas transmission, hydroelectricity, and wholesale power markets. NERC, a not-for-profit, non-governmental body charged with organizing the voluntary reliability efforts of electric utilities in nine regions across the U.S., was established as a direct result of the massive 1965 New York blackout. The Energy Policy (EP) Act of 2005 created a new hybrid approach to system reliability with designation of an Electric Reliability Organization (ERO) to establish mandatory standards governing operations and information pertaining to the electric utility industry. In 2007, FERC designated NERC as the national ERO responsible for writing standards, while FERC retained its authority to review and approve those standards.

---

[27] The National Infrastructure Protection Plan is a Department of Homeland Security document which outlines how government and the private sector can partner to develop protocols to protect critical infrastructure. Resiliency refers to the ability of the electric grid, or any system, to prepare for and adapt to serious stressors such as physical attack or severe weather events.

[28] Kolasky Interview with Eric Holdeman in *Emergency Management* magazine, March 21, 2014. See *http://www.emergencymgmt.com/safety/Sharpening-the-Focus-on-Critical-Infrastructure.html*

[29] Fischer, Eric, *Federal Laws Relating to Cybersecurity, Overview and Discussion of Proposed Revisions*, Congressional Research Service, June 13, 2013.

Even before EP Act 2005, both entities had undertaken approaches to regulating critical infrastructure. Immediately after 9-11, FERC began promulgating rules on Critical Energy Infrastructure Information (CEII) that severely limited, then refined, the ability of the public and market participants to access materials like maps and documents that could provide sensitive information about grid vulnerabilities.[30]

NERC's efforts to create new, largely voluntary, standards for the power system took the form of various Critical Infrastructure Protection (CIP) standards. Beginning in 2005, NERC members worked on, and then forwarded for FERC approval, nine initial CIPs, which have become mandatory and subject to NERC enforcement:[31]

- **CIP-001:** Covers sabotage reporting;
- **CIP-002:** Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System;
- **CIP-003:** Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets;
- **CIP-004:** Requires that personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness;
- **CIP-005:** Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter;
- **CIP-006:** Addresses implementation of a physical security program for the protection of Critical Cyber Assets;
- **CIP-007:** Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters;
- **CIP-008:** Ensures the identification, classification, response, and reporting of cybersecurity incidents related to Critical Cyber Assets; and

[30] See FERC's web site for a listing of major CEII regulations, *http://www.ferc.gov/legal/maj-ord-reg/land-docs/ceii-rule.asp*

[31] NERC CIPs do not apply to nuclear energy facilities, which are under jurisdiction of the Nuclear Regulatory Commission.

- **CIP-009:** Ensures that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

CIP standards undergo regular modification. On November 22, 2013 FERC approved CIP Version 5 which includes significant changes and additions to the existing collection of standards.[32] The changes are scheduled to become enforceable in 2016.

As of early January 2015, CIP-010, *Configuration Change Management and Vulnerability Assessment* and CIP-011*, Information Protection,* as well as CIP-014*, Physical Security,* are standards subject to future enforcement.[33]

Until the recent adoption by FERC of CIP-014, which is specific to critical facilities in the bulk power system, including substations, but not electric generators,[34] CIP-004 and CIP-006 had the most impact on physical aspects of security. FERC's initial directive to NERC to formulate these physical security standards indicated that a major component of the rules would be for owners and operators of the grid to perform risk assessment of their system and identify facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnected grid through instability, uncontrolled separation, or cascading failures.

FERC recognized that "critical" facilities would be a relatively small subset of all facilities that comprise the electric grid. "[Of] the many substations on the bulk power system, our preliminary view is that most of these would not be 'critical' as the term is used in this order. We do not expect that every owner and operator of the bulk power system will have critical facilities under the reliability standard…"[35]

The standard requires that owner/operators of the grid "develop and implement a security plan to protect against attacks on these facilities."[36]

---

[32] FERC. *Order No. 791 Final Rule.* http://www.ferc.gov/whats-new/comm-meet/2013/112113/E-2.pdf
[33] NERC. *Standards Subject to Future Enforcement.* http://www.nerc.com/pa/Stand/Pages/StandardsSubjecttoFutureEnforcement.aspx?jurisdiction=United States
[34] RM14-15-000, approved with modification November 20, 2014.
[35] RD14-6-000; March 7, 2014, 146 FERC ¶61,1666 at P.11
[36] FERC news release July 17, 2014.

4.2. Other Physical Security Standards

Outside of the national regulatory arena, the electric power industry is looking to develop physical security standards for substations, regardless of whether they are part of the bulk power system or local distribution networks not under FERC jurisdiction.

The Institute of Electrical and Electronics Engineers (IEEE), a professional association founded in 1963, is responsible for developing many standards for equipment and practices used by the electric utility industry, including the widely recognized IEEE 1547 standard for safety of all devices that are interconnected to the grid.

As of January 2015, IEEE members are developing P1402, a Standard for Physical Security of Electric Power Substations. The standard would "define sound engineering practices for substation physical protection that could be applied to . . . substations that are unmanned, and thus susceptible to unauthorized access, theft and vandalism."

The prospective standard is mostly concerned with issues of access, monitoring and delay/deter features to mitigate vulnerability at such facilities. P1402 "does not establish requirements based on voltage levels, size or any depiction of criticality of the substation" but rather leaves it up to the facility owners to determine applicability to their assets.

4.2.1. Other Industry Standards

Several existing industry standards not specifically related to physical security are nonetheless relevant. These include National Fire Protection Association (NFPA) and National Electric Safety Code (NESC) standards, as well as International Organization for Standardization (ISO) standards such as ISO 55000 (Asset Management Standard), ISO31000 (Risk Management Standard), and ISO 9001 (Quality Management Standard).

4.3. Existing CPUC Regulation and Oversight Activities

Commission policies and regulations have long included provisions related to electric grid physical security. Commission staff regularly inspects and investigates existing security measures at electrical facilities. During inspections of power plants, underground and overhead facilities and

substations under General Orders 174, 165, 167, 128 and 95,[37] Commission staff verifies the condition and operation of existing physical security protections such as substation fences and lighting, padmount locks, vault covers, and electric generating station security plans.
The Commission evaluates security measures as part of electric utility rate cases. CPUC policies now require the utilities to discuss both safety and risk assessment in every rate case. Commission staff annually review electric utility emergency plans, and regularly monitor utility emergency exercises as required by General Order 166.[38] In addition, Commission staff investigates incidents related to security at electrical facilities, including both the 2013 Metcalf gunshot attack and the 2014 Metcalf security breach and burglary.

4.3.1. Metcalf Attack and Metcalf Burglary

On April 16, 2013, a gunshot attack damaged several high voltage transformers and other equipment at Pacific Gas and Electric's Metcalf Transmission Substation south of San Jose. No customers lost power and no injuries were reported, but the cost of repairs approached $15.4 million, and the attack rendered the substation inoperable for approximately one month. Following this attack, PG&E initiated several changes to its security protocol at this substation.

Despite these changes, between the hours of 22:10 on August 26, 2014, and 02:41 on August 27, 2014, burglars cut through the fence at the Metcalf Substation and removed tools and equipment valued at $38,651.[39]

Law enforcement personnel[40]investigated both incidents with a goal of identifying and apprehending the perpetrators. At the same time, staff from the Commission's Safety and Enforcement Division (SED) investigated the incidents to evaluate PG&E's security measures and compliance with Commission regulations.[41]

Following the 2014 Metcalf burglary, SED directed PG&E to conduct a root cause analysis (RCA) into the event. Although the full RCA report is confidential, PG&E prepared a non-confidential

[37] General Order 95, "Rules for Overhead Electric Lines"; General Order 128, "Rules for Construction of Underground Electric Supply and Communication Systems"; General Order 165, "Inspection Requirements for Electric Distribution and Transmission Facilities"; General Order 174, "Rules for Electric Utility Substations"; General Order 167, "Enforcement of Maintenance and Operation Standards for Electric Generating Facilities."
[38] General Order 166, "Standards for Operation, Reliability, and Safety During Emergencies and Disasters."
[39] PG&E. *Metcalf Root Cause Analysis Summary report*. November 21, 2014, p2.
[40] Including local police for both incidents and the FBI for the April 2013 gunshot attack.
[41] SED's investigation of the August 26-27, 2014 incident is on-going.

summary document showing its analysis of the causes and major action items it is undertaking in response to both the 2013 attack and the 2014 break-in (See Appendix B).

4.4 Physical Security Activities in other States and Power Agencies

Our research indicates California leads the way in efforts to improve electric grid physical security. However, some other states and power agencies have undertaken noteworthy efforts in this area.

Arizona has a history of both grid security events and utility action in response to these events. In 2007, security working at a checkpoint stopped a worker carrying a pipe packed with firework explosives. In February of 2014, target shooters in the vicinity of a Nogales substation were confronted by plant security and law enforcement. In June of the same year, saboteurs detonated a makeshift explosive device near spare oil tanks at a substation in the same general area. Law enforcement investigated all of these incidents. In March 2014, in the wake of the Metcalf attack, the Arizona Corporation Commission sent a letter to state utility owners asking about planned improvements to mitigate physical security threats in their facilities.[42]

Arizona utility activities in the security area predate these events. In 2000, the FBI established an advisory program on substation grid physical security for Arizona utilities. Under the "infragard" program, the federal government shares security information with electric corporations in the state.

Pennsylvania Utility Code 52 Chapter 101 requires all jurisdictional utilities to prepare physical and cyber security plans as part of their emergency preparation, and to self-certify that those plans meet state requirements.[43]

The Bonneville Power Administration, a federal power agency operating in the Pacific Northwest, has conducted hundreds of security and risk assessments since 2001, and in 2014 proposed an additional $37 million in capital spending for physical security measures at its critical substations.[44]

In 2014, Dominion Virginia Power Company proposed increased expenses over five to seven years to harden critical infrastructure against man-made threats. Dominion's efforts, which began in 2013 at the most critical substations, included typical physical security improvements; additional

---

[42] *Sabotage puts Focus on Threats to the Grid.* AZcentral. June 12, 2014. See http://www.azcentral.com/story/news/arizona/2014/06/12/sabotage-nogales-station-puts-focus-threats-grid/10408053/
[43] Pennsylvania Public Utility Code 52, Section 101. *Public Utility Preparedness Through Self Certification.*
[44] Parformac, op cit p.21.

access control and improved physical barriers, equipment hardening, polymer bushings, and spare equipment stored offsite.[45]

In February of 2012 the Tennessee Valley Authority began increasing security at its non-nuclear infrastructure, stationing 24-hour contract guards at critical facilities, as well as improving its surveillance method including video analytics, infrared monitoring, and enhanced coordination with local law enforcement agencies.[46]

An interesting problem in western Africa is the theft of transformers for cooling oil, which residents of the area use for a wide variety of purposes including cooking and as a salve for wounds. In 2012 Kenya Power spent about seven percent of its profits replacing transformers, which led them to begin locating transformers in homes, higher up on poles, and in other inaccessible areas.[47]

5.0. Examples of Physical Security from Other Industries

Although different industries may have different specific concerns, and different assets to protect, the methodologies used in security planning, and the types of protections available are very similar to those employed in the electric industry. Some notable examples are described in this section.

5.1. Physical Security in the Nuclear Industry

In addition to the common threats to electrical reliability, the nuclear industry faces unique challenges because of the need for a nuclear protective system to safeguard the fissile material. Access to all nuclear plants is strictly controlled with armed guards, fences, and advanced intrusion detections. Since the terrorist attacks of September 11, 2001, the nuclear industry has concerned itself with large airplane crash attacks.

In performing their risk and threat assessment, nuclear generators divide their plants into concentric areas of escalating security, from the outer perimeter or "owner controlled area" down to the

[45] Parformac, op cit p.20.
[46] Parformac, op cit p.19.
[47] *Thieves Fry Kenya's Power Grid for Fast Food.* Aljazeera. December 28, 2014. http://www.aljazeera.com/indepth/features/2014/12/thieves-fry-kenya-power-grid-fast-food-2014122884728785480.html

central vital area which houses the actual nuclear material and critical controls. To protect these areas, the industry uses various tools, including physical barriers, electronic surveillance, bullet-resisting protected positions, background checks and specialized security forces.[48]

5.2. Physical Security in the Chemical Industry

In 2009, the Department of Homeland Security (DHS) worked with the chemical industry to develop a set of anti-terrorism standards. The product of this collaboration is a collection of physical security risk based performance standards and metrics for evaluating the implementation of those standards. The Chemical Industry divided asset protection and security strategy into three main areas:

1. Physical security
2. Cybersecurity
3. Security Policies, Procedures and Plans

The Chemical industry plan defines physical security narrowly, to include (1) perimeter barriers; (2) monitoring and intrusion detection systems; (3) security lighting; and (4) security forces.[49]

Other entities may take a more expansive view of the definition of physical security to include elements of cybersecurity, information security, and policies, procedures and plans.[50]

5.3. Physical Security for the Financial Sector

The financial sector utilizes the same sorts of physical security strategies as the other industries discussed above. Layered defenses are used around critical assets and structures such as buildings and data centers. These defenses include deterrent and delaying devices such as walls, locks and access controls, detection devices, and policies and procedures for access, as well as security forces when needed.[51]

---

[48] Nuclear Energy Institute. Physical Security. http://www.nei.org/Master-Document-Folder/Backgrounders/Fact-Sheets/Nuclear-Power-Plant-Security

[49] Department of Homeland Security (DHS). Risk Based Performance Standards Guidance. Chemical Facility Antiterrorism Standards. May 2009, p148.

[50] Part of the Commission's task in enforcing Senate Bill 699 will be determining what falls under the rubric of "physical security."

[51] *Enterprise Risk Management*. PCI Security Systems. 2014. See http://www.emrisk.com/knowledge-center/newsletters/physical-security

5.4. Military Physical Security

Army field manual FM 3-19.30 spells out security measures for army facilities. Not surprisingly, the field manual lists common physical security measures such as Protective Barriers, Lighting, Electronic Systems, and Access Control.[52] The field manual recommends a system based approach including risk, threat and vulnerability assessment.

6.0. Risk Based Physical Security for the Electric Grid

6.1. Risk Management Process

The risk management process is an accepted methodology used either implicitly or explicitly in most threat prevention strategies.

The Risk Management Process[53]

Typically, risk management involves a process of risk and vulnerability identification and assessment, risk mitigation or control, and a monitoring process based on performance standards. Without divulging the specific activities of any particular utility, discussions at both the open and

[52] *Army Field Manual FM3-19.30*. 2001. See https://www.wbdg.org/ccb/ARMYCOE/FIELDMAN/fm31930.pdf
[53] *Risk Management.* Suwanee County Florida. See http://www.suwcounty.org/index.php?option=com_content&view=article&id=32&Itemid=67

closed sessions of the CPUC June 2014 physical security workshop indicated that all utilities use some sort of risk and vulnerability assessment to plan for physical security protections, and utilize similar physical threat mitigation techniques.

6.2. Risk Identification and Assessment (Evaluate Risks, Threats, and Vulnerabilities)

The first step of a risk based process is the identification of all potential risks, threats and vulnerabilities, then the classification or assessment of these risks. In assessing risk, evaluators look at all potential threats, analyze the vulnerabilities of equipment to those threats, evaluate the likelihood and impact of an event occurring related to that threat, and assign a risk priority to the threat.

Some risk evaluators use tools developed to identify and access threats. One such tool is the so-called CARVER matrix, developed by Special Forces during the Vietnam War.[54] The acronym CARVER stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability.[55]

In the electric industry, threats can be classified by the source and the methodology. As to the source of physical risks and threats, they can potentially emanate from vandals or thieves, disgruntled employees and possibly terrorist entities. The methodology of attack can include vehicle (land or aerial) attack, human intrusion for purposes of damaging or stealing equipment, gunshots, bombings or attacks with other weapons.[56] Advanced modern forms of attack could potentially include electromagnetic pulse weapons which can disrupt grid operations. As part of this threat identification process, and throughout the risk management process, the utility will also look at the vulnerability of the assets to different types of attacks.

---

[54] Tucson Electric Power used this methodology in developing its plan for compliance with NERC CIP 14. Tucson Electric Power Presentation, September 2014.

[55] Bennett, Brian T. (2007). *Understanding, assessing, and responding to terrorism: protecting critical infrastructure and personnel* (2007 ed.). John Wiley & Sons. ISBN 0-471-77152-X.

[56] A representative from Lawrence Livermore Laboratories, commenting at the 2014 CPUC substation workshop, indicated that while possible, bombings of substations were less likely than other modes of attack.

After enumerating all potential risks, the utility will classify the risks according to probability of occurrence and severity of impact. This type of assessment generally leads to the development of a risk matrix.[57]

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Risk Matrix

Probability considerations include (but are not limited to):

1. Geographical location
2. Ease of access, vulnerability of asset to attack
3. Criticality or importance of asset to the delivery system
4. Local demographics
5. Existing natural barriers
6. National security intelligence and reports, current security climate

The probability of some specific risks may depend on specific unique factors. Copper theft is always a major issue for utilities at the distribution level. Not only does this theft involve a large loss of property, but vandals are frequently killed or injured stealing copper. As a result, twenty six states have considered legislation to reduce or prevent copper theft, primarily by controlling the businesses that reclaim copper.[58] Despite the fact that copper theft is always a problem for utilities, the probability can be tied to specific external factors such as economic conditions and the cost of copper. All of these factors should be included in a risk management probability assessment.

[57] *Risk Management.* AcQNotes. 2014. http://www.acqnotes.com/Tasks/Element-3-Assess-and-Document-Risk.html
[58] *Copper Theft Survey*. Electric Safety Foundation International. 2014. See http://esfi.org/index.cfm/page/ESFI-Releases-Results-of-National-Utility-Copper-Theft-Survey/cdid/10357/pid/10262

To evaluate the severity or the impact of a successful attack, security planners consider the potential impact of loss of a particular asset. Potential results of a successful physical attack on distribution facilities can include death or injury to the public or workers, financial loss through equipment replacement, health and safety ramifications due to loss of power or stability in the electric system. Some impacts, such as financial loss, can be relatively easily quantified. Others are less tangible. To determine the likely potential impact of attack on a specific facility or asset, considerations should include (but are not limited to) the following.[59]

1. Type of facility- generation, substation, transmission or distribution,
2. Criticality of facility to operation of the grid,
3. Criticality of the facility based on customers,
4. Ease of restoration of the facility, replacement spares, cost of replacement,
5. Ability of the grid to function normally given loss of the particular asset (redundancy or resiliency concerns). These redundancy or resiliency concerns include the difficulty of repair, the availability of alternative paths in the grid, presence of effective remedial action schemes, and the availability of spare parts.

In general, the threat considerations and mitigation techniques for generating stations would be similar to those for substations. Generating stations contain physically larger targets (such as boilers) and large transformers, in particular the main step-up transformer, but are more likely to be manned and guarded. Additionally, according to NERC, although it may have a significant effect on local reliability, the loss of one generator is typically not as damaging to grid stability as the loss of a critical transmission substation.[60]

6.3. Risk Mitigation (Control Risks)

6.3.1. Physical Mitigation

6.3.1.1. Mitigating Threats to Substations

Physical mitigation of threats to electric facilities includes deterrence or prevention, detection, and response. As discussed above, the Department of Homeland Security, in planning for the Chemical Industry, defined physical security narrowly, to include perimeter walls and fences, intrusion

[59] CPUC Substation workshop discussions, June 2014.
[60] FERC. *Notice of Proposed Rulemaking. Docket RM14-15-00.* July 17, 2014. P22.

detection, lighting and security forces. Expanding on that narrow definition, it is possible to delineate general areas of physical security measures under the headings of deterrence, detection, and response.

- *Deterrence (or prevention) includes, but is not limited to:*
    - Walls, gates, locks and fencing (consider whether intrusion will be by human or vehicle and what types of vehicles might intrude)
        - Layered concentric approach
        - Surrounding entire substation or individual equipment
        - Chain link, concrete, vinyl, metal, wood, barbed wire, razor wire, cinder block, block, cables
        - Opaque fencing or walls to prevent visual sighting of substation equipment
    - Signage
        - High voltage signs, guard signs, signs indicating existence of cameras
    - Guards
        - Manned stations, patrolling, specially trained guards
    - Lighting
        - Properly designed lighting both deters intruders and makes intruders easier to identify
    - Vegetation management
        - Removal of attacker concealing shrubbery from perimeter of substation, removal of shrubbery from substation fencing.
- *Detection (Monitoring) includes:*
    - Cameras
        - Video, pan-zoom-tilt, inward pointing or outward pointing[61]
    - Intrusion detection
        - Infrared, Motion sensors, fence mounted, beam sensors, open area sensors, acoustic
    - Gunshot detection
    - Aerial surveillance, manned or unmanned

[61] As part of its strategy following the Metcalf incident, Pacific Gas and Electric decided to change its focus to increase both inward and outward pointing cameras to detect threats. Substation Workshop Comments, June 2014.

- Analysis of unusual or increased traffic patterns or other activity near electrical assets
- Equipment alarms (in conjunction with intrusion or gunshot detection can indicate presence of attack or malevolent actor)
    - Low oil alarms (can indicate gunshot), temperature alarms, ground fault alarms
    - Gate or door alarms
    - Alarm interpretation and integration systems, control centers to eliminate human error

In addition, utilities may need systems to interpret alarms from detection equipment. For example, a detected gunshot followed immediately by some sort of equipment failure alarm may represent gunshot damage to a piece of equipment. Similarly, an intrusion alarm followed by an equipment alarm may indicate a vandal removing equipment or copper. In these instances cameras can also be used to attempt to identify the exact nature of the attack.

- *Response (minimize effects of attack)*
    - Advanced technology
        - Self-sealing transformer, hardened equipment and cooling systems, gunshot resistant polymer bushings
    - Improving Resiliency
        - Multiple alternate paths for delivery of electricity
        - Effective remedial action schemes to minimize effect on other facilities
    - Improving Restoration[62]
        - Ready spares
        - Cooperative agreements for manpower and equipment sharing with other utilities.
        - Advanced communication systems (SCADA, microwave)
        - 24/7 monitoring of alarms

[62] The CPUC staff report on the 2011 Southern California Windstorms, *Investigation of Southern California Edison Company's Outages of November 30 and December 1, 2011*, recommended several areas of improvement for Southern California Edison's (SCE's) emergency response procedures. Additionally, CPUC General Order 166 requires utilities to prepare emergency response reports.

- Drills with local first responders
- Emergency planning
    - FEMA Incident Command System (ICS) and National Incident Management System (NIMS) training and programs

6.3.1.2. Mitigating Threats to Overhead and Underground Facilities

In a February 2014 article on the PG&E Metcalf Substation attack, the *Wall Street Journal* reported:

> "Overseas, terrorist organizations were linked to 2,500 attacks on transmission lines or towers … from 1996 to 2006, according to a January report from the Electric Power Research Institute."[63]

In the United States, underground and overhead electric facilities regularly sustain damage from vandals and thieves, if not from terrorist entities. However, sophisticated mitigation and prevention is not as critical because spares and repair staff are nearly always available. With exceptions, electric utilities also maintain some redundant paths for delivery of power at the transmission and distribution levels.

A 2006 California "heat storm" which resulted in overheating damage to numerous distribution transformers, and a 2011 windstorm in Southern California demonstrate that widespread damage to overhead or underground distribution facilities can cause extended outages and significant restoration costs. However, the sheer number of these facilities renders them difficult to protect, while the availability of more attractive targets such as substations makes overhead and underground distribution facilities less likely to sustain a terrorist attack. Rather than trying to completely protect each pole or tower, utilities typically concentrate on maintaining spares and developing effective restoration plans.

Still, some cost effective mitigation efforts are advisable, and in some cases mandated by existing Commission rules, specifically General Orders 95 and 128. These security mitigation efforts also help from a safety standpoint. Typical mitigation efforts for these facilities include:

---

[63] Smith, Rebecca. "Assault on California Power Station Raises Alarm on Potential for Terrorism." *Wall Street Journal*, February 5, 2014.

- Removing pole steps to make poles more difficult to climb
- Climbing guards on tower and lattice structures
- Locking devices on pad mounted transformers and switches
- Fasteners on vault covers
- Over-insulation on transmission towers including oversized or redundant insulators and gunshot resistant polymer insulators
- Signage warning of shock hazard or in some cases surveillance

Additionally, given the existence of important, high capacity submarine cables, such as the Trans-Bay cable, utilities should include the protection of these assets in their security plans where applicable.

6.3.1.3. Spare Parts Programs and Planning

An electric substation typically consists of transformers; circuit breakers and relays, which provide protection for the power lines and substation equipment; batteries for back-up and to operate the relays; and other ancillary switches, buses and equipment. Because a substation contains large pieces of important equipment in a centralized location, it could be an attractive target for thieves, vandals, and other malevolent actors. The substation power transformers are of particular concern in security planning because they are critical to the operation of the substation, are large targets, with several areas of vulnerability (bushings, oil tanks, controls), in general are unique to the substation, are costly and require large leads times for replacement. According to the United States Department of Energy, lead times for high voltage transformer replacements can vary from 6 to 20 months, and each transformer replacement can cost over 10 million dollars each.[64]

For large items such as transformers, utilities may maintain formal and informal sharing and cooperative arrangements with each other. Some formal sharing agreements also exist under the NERC Spare Equipment Database and Edison Electric Institute Spare Transformer Equipment Program.[65]

Other assets in the electric system include poles, towers, lines, bushings, small transformers and capacitors, and associated equipment. For such equipment in the lower voltage distribution system,

[64] Parfomak, op cit., p 4.
[65] Electric Power Research Institute. *Power Transformer Emergency Spares Strategy*. October 2014.

utilities typically maintain a significant number of spares. Additionally, distribution level parts do not typically present the logistic and lead-time problems associated with transmission level equipment.[66]

6.3.2. Policies and Procedures Related to Physical Security

Utility policies and procedures should support the physical security measures. These policies and procedures include background screening of personnel, training, access control processes, and drills and exercises.

Given the complexity of modern technology used in security systems, training of guards and security control center personnel is crucial. Additionally, these security employees (or contractors) must be provided with clear policies and procedures. PG&E's summary report on the causes of the breakdown in security during the Metcalf burglary identified training and updated procedures as key action items.[67] All training programs and policies should be reviewed regularly. Training programs should include employee testing, and retesting on regular basis, and must include provisions that stimulate real-world scenarios if possible.

All protection equipment such as alarms, intrusion detectors, lights, and cameras should be properly maintained and tested frequently. Thorough preventive and predictive maintenance programs should be developed for the security of such equipment. Some testing and inspection should be performed as part of routine substation inspections. To dissuade thieves and vandals, valuable material should never be stored in plain sight in a substation.

6.3.3. Other Considerations for Risk Mitigation Planning

6.3.3.1. Cost Considerations

Any security mitigation plan must take into account the costs involved. In particular, for investor owned utilities which must recoup costs through rate mechanisms, it is important to consider the cost of security measures to the end customer. Tall walls, large security forces and advanced technology might provide the ultimate in security but in many cases will be excessive, and will present an untenable burden, particularly to low income residential customers.

---

[66] Discussion at physical security workshop. CPUC. June 2014.
[67] PG&E. *Metcalf Root Cause Analysis Summary report*. November 21, 2014, p6.

As part of that consideration, the utility must not only take into account the nature of threats and the type of facilities it owns, but the nature of its rate base and the cost which the customers can support. Every decision should include the consideration of multiple alternatives, and a cost-benefit analysis. Some costs, such as the price of a wall or the actual replacement cost of an asset damaged by a successful attack, are clear. Tools and rubrics exist for calculating the numerical cost of loss, including Annual Loss Expectancy calculations.[68] Devastating losses, such as loss of life, and other intangible losses, such as organization reputation, are more subjective. Accounting models exist for comparing alternative expense choices and evaluating long and short term costs as well as opportunity costs.

For example, in Southern California Edison's (SCE's) 2015 rate case, SCE analyzed the costs and benefits of utilizing advanced security guards, compared to an alternative approach of utilizing some security guards along with detection equipment and software analysis.[69] SCE determined it could achieve significant savings without sacrificing security by using the combined approach.

Finally, when utilities perform risk-benefit studies, they may perform more comprehensive analysis, considering security risks as part of the entire constellation of risks to service, such as extreme weather events, earthquakes, or failure of other facilities which may affect the performance of the facility in question.[70] The CAISO typically performs its reliability studies in this manner.

6.3.3.2. Environmental Impact Considerations

Investor-owned utilities are required to obtain permits from the CPUC for construction of certain specified infrastructures listed under Public Utilities Code (PU Code) sections 1001 et seq., including distribution facilities.[71] Typically, as part of the CPUC's permit application review and decision-making process, the CPUC, as the lead agency, conducts an environmental review

[68] Malashenko, Villareal and Erikson. Cybersecurity and the Evolving Role of State Regulation: How it Impacts the California Public Utilities Commission. September 19, 2012, p3.
[69] SCE General Rate Case 2015 Testimony. SCE-07, Volume 4, p 41.
[70] For example, failure of a gas delivery system may affect the reliability of a power plant. These considerations are known as "co-located facility" considerations.
[71] The CPUC reviews permit applications under two concurrent processes: (1) an environmental review pursuant to the CEQA, and (2) the review of project need and costs pursuant to PU Code sections 1001 et seq. and General Order (G.O.) 131-D (Certificate of Public Convenience and Necessity (CPCN) or Permit to Construct (PTC)).

pursuant to the California Environmental Quality Act (CEQA).[72] The CEQA process requires the lead agency to identify potentially significant environmental impacts to several impact areas, and to avoid and/or mitigate any environmental impacts found to be significant. If the CPUC approves the permit application, it issues a decision approving the construction, which would adopt environmental mitigation measures and a mitigation monitoring plan.

This section discusses common CEQA environmental mitigation measures related to distribution facility and substation projects that may need to be considered in utility distribution system physical security planning. One should keep in mind that CEQA mitigation measures are project specific and the discussion in this section is a general approach to environmental consideration when developing physical security plans. When assessing environmental impacts under CEQA, it is often determined that the introduction of a new land use, such as a substation, to the project area would result in land use changes/impacts as well as potential long-term visual quality impacts to the surrounding area. Generally, a new substation would result in the degradation of existing visual character/quality of the substation site and its surrounding area, or the creation of a new source of light or glare that would adversely affect day or nighttime views in the substation area.[73]

Common environmental mitigation measures for preserving existing visual character/quality require the project proponent to establish a landscaping and maintenance plan for a permanent vegetative screening and to coordinate with local land use planning department/agencies to ensure consistency with applicable visual resources goals and policies. The following common mitigation measures could be part of the landscaping and maintenance plan developed by the project proponent and submitted for review and approval by the relevant local agency, such as the city, county, or other agency with land use jurisdiction:

- Vegetative screen of sufficient height and density to provide for visual screening around the substation and all substation components, consistent with safety, feasibility, and engineering requirements.
- Visually opaque gate at substation entrance to obscure views through the gate from the substation site entrance road.

[72] The CEQA Guidelines are codified at Title 14 California Code of Regulations section 15000 et seq.
[73] Appendix G of the CEQA Guidelines identifies the circumstances that can lead to a determination of a significant impact.

- A perimeter wall of sufficient height to obstruct views into the facility, in addition to exterior landscaping.

To address the environmental impacts created by a new source of light or glare from the substation that would adversely affect day or nighttime views in the project area, mitigation measures for light and glare might ensure all lighting is shielded, directed downward, and of minimum brightness necessary for safety, and that no direct or excessively bright reflective light would be present off-site, as follows:

- Shroud and minimize unnecessary sources of light: Design and install new permanent substation lighting such that light bulbs, lenses, and reflectors would not be visible from public viewing areas so that the lighting does not cause reflected glare and that illumination of the project, vicinity, and nighttime sky is minimized.

    a. Lighting could be designed so exterior light fixtures are hooded where possible, with lights directed downward or toward the area to be illuminated and so that backscatter to the nighttime sky is minimized.

    b. Design of the lighting could be such that the luminescence or light source is shielded to prevent light trespass outside the project boundary.

- Lighting could be restricted to the minimum necessary brightness consistent with worker safety and Occupational Safety and Health Administration (OSHA) requirements.

- Lighting could be kept off when the site is unoccupied in order to minimize nighttime sky illumination, and could only be switched on during the nighttime in order to perform maintenance or outage repairs.

As stated above, this discussion is intended to be general and to highlight common environmental mitigation measures that may need to be considered as part of physical security planning for distribution facilities. However, as part of the rulemaking for rules for distribution physical security, the CPUC may ask the parties to review CEQA documents and other sources to determine other applicable environmental impacts and mitigation measures for consideration.

We note that, in a CEQA review, the safety impacts of potential environmental mitigation measures should be an important consideration in assessing their feasibility. With the increased emphasis on physical security, perhaps there will be creative developments in measures that mitigate environmental impacts without creating security concerns.

6.3.3.3. Miscellaneous Considerations

Some other considerations in development of physical security plans include local geography and demographics, customer base, facility design, environmental rules and considerations beyond CEQA requirements, local codes including aesthetic considerations, and the population in the vicinity of electric facilities.

To incorporate these considerations, the utility should use sound engineering judgment, experience and consider the national security climate.

6.4. Metrics (Review Controls)

The risk management process is a dynamic methodology. Along with identifying and assessing risk and developing and implementing a mitigation strategy, security planners should develop a set of metrics to determine if their strategy is optimal, and use these metrics to make strategic adjustments where necessary. The use of metrics also becomes critical in the context of regulation which will be, at least to a certain extent, performance based.

6.4.1. Prescriptive versus Performance Based Regulations

In general, two possible models exist for regulation – a strict prescriptive approach, or a performance based approach. Under a prescriptive approach, the regulation requires the utility (or other regulated entity) to comply with specific design or operational requirements. In other words, the regulation dictates exactly what actions the utility must take to remain in compliance, and exactly "how" the utility should perform these actions. In a performance based regulatory structure, the regulation does not specifically detail "how" the utility must comply, but requires instead that the utility must address a certain issue (such as physical security or environmental requirements), and must meet certain performance metrics.

For example, a prescriptive environmental regulation might require all electric generators to be built with selective catalytic reduction equipment to control emissions. A performance based requirement might require the utility to develop an emission control plan that reduces emissions to a certain level or by a certain amount.

Electric distribution systems differ immensely from one utility to another. Geography, weather, local construction codes, size of territory, demographics of area, types of customers, and design of substations and other facilities vary significantly, particularly between small, mainly rural utilities and larger, urban utilities.

Because the nature of utility physical security is not one-size fits all, a prescriptive approach can have some major deficiencies:

- Some prescriptive requirements might be applicable to some facilities and not others,
- Security, technology and best practices rapidly evolve. Prescriptive rules could impose inefficient, ineffective, and out-of-date requirements,
- Prescriptive requirements may not address significant new threats,
- Prescriptive requirements could require almost constant revision.

For these reasons, a performance based approach is often more effective than a prescriptive approach. Under a performance based approach, the compliance of the security plan is based on how well the implemented plan meets metrics established by either the utility itself or a regulating body.

6.4.2. Control Metrics for Utility Distribution Systems

Control metrics can include both quantitative or statistical metrics and qualitative performance metrics. Examples of *quantitative* metrics for distribution physical security measures include tracking copper theft, successful or unsuccessful intrusion or attack, false or nuisance alarms, condition of all monitoring equipment, performance of security personnel in training exercises and on tests, results of substation inspections including number of problems found with condition of deterrence and monitoring measures, instances of vandalism or graffiti, problems with access control, number of malfunctions of security equipment, or camera coverage. Of course, any

attempted or successful attacks should be reflected in the metrics. Resiliency and restoration capabilities can be tracked through outage restoration time data and asset loss simulations.[74]

One example of *qualitative* metrics is using a subjective expert analysis to compare a planned or existing protection scheme to a developed standard metric. For example, for efforts to detect threats, the Chemical Industry compares programs to various standard "tiers" of acceptability. The industry describes the lowest "tier" of acceptability (Tier 4) as:

> *The facility has some ability to detect attacks at early stages.*

The highest tier (Tier 1) is presumably the "gold-standard" in attack detection. The Chemical Industry describes this level of protection as:

> *The facility has a very high likelihood of detecting attacks at early stages through countersurveillance, frustration of opportunity to observe critical assets, surveillance and sensing systems, and barriers or barricades. To achieve this level of detection, a facility could, for example, maintain a facility-wide intrusion detection system that is continually monitored from a Security Operations Center and has an adequate backup capability.*[75]

In addition, utilities can develop various test scenarios or exercises and evaluate the performance of their security systems under stress. These can include both tabletop and actual attempts to breach the security system to determine its effectiveness. Because large scale attacks are rare, the utility should simulate attacks or other actions such as third party surveillance of a station or other asset, and record quantitative metrics from these tests.

Finally, an analysis of any security related findings from facility insurance inspections (often conducted by independent security and risk experts) or internal utility audits can provide both quantitative and qualitative indications of the effectiveness of existing security measures.

---

[74] Evaluating utility benchmark outage data such as the Customer Average Interruption Duration Index (CAIDI) can provide an indication of potential restoration time after any event.
[75] Department of Homeland Security (DHS). op cit. p 58.

7.0. Proposed Next Steps for the Commission

As stated above, existing Commission rules have long addressed electric distribution system physical security. The attacks on the Metcalf Substation make it apparent that there is a broader role for regulatory oversight in this area. Because of new state requirements pursuant to Senate Bill 699, the path forward for the Commission is somewhat clear, at least initially. Senate Bill 699 (amending Public Utilities Code Section 364) requires the Commission, by July 2015 to initiate a proceeding to develop rules for addressing physical security risks to the distribution systems of electrical corporations. Section 364 further states (in part),

> *The standards or rules, which shall be prescriptive or performance based, or both, and may be based on risk management, as appropriate, for each substantial type of distribution equipment or facility, shall provide for high-quality, safe, and reliable service.*

and,

> *In setting its standards or rules, the commission shall consider: cost, local geography and weather, applicable codes, potential physical security risks, national electric industry practices, sound engineering judgment, and experience.*

7.1. Development of Rules Required by Senate Bill 699

7.1.1. Potential Model for Rules for Physical Security

Given differing geographical locations, designs, cost considerations, and other factors, it would be imprudent to rely solely on prescriptive "one-size fits all" physical security requirements for distribution[76] facilities for all electric utilities. Instead, a risk based-performance approach, similar to that seen in the chemical industry, is one feasible approach.[77]

[76] Note that while Section 364, mentions the "distribution" system, the statute does not define the term. As part of the rulemaking process, the Commission should decide what sorts of facilities the new rules apply to. This could include all substations and power lines at all voltage levels, as opposed to only those lower voltage facilities typically considered as "distribution" assets.

[77] What is presented here is only one potential model for enforcement of the changes to PUC Section 364 under Senate Bill 699. The final decision will be based on a rulemaking proceeding, potentially with stakeholder workshops.

Electric utilities already evaluate risks in security planning. It is likely that all electric utilities will consider similar threats and risks, and utilize similar considerations (cost, resiliency, restoration difficulty) in evaluating those threats.

However, because the Commission has certain mandates from new and existing legislation, along with certain established priorities (e.g., cost considerations and environmental protection), a hybrid plan, including risk based performance rules with some general semi-prescriptive guidelines, may be optimal.

The new NERC CIP-014-1 standard, along with the processes developed under CPUC General Order 174 for Substation Inspections and CPUC General Order 167 for Power Plant Operations and Maintenance present good potential starting points for an enforcement model.

Under NERC CIP-014-1, bulk power transmission owners are required to identify critical substation assets, identify and assess risks to those assets and develop a unique physical security strategy to mitigate those risks. The NERC standard mandates that each step in the process be vetted by an independent expert.

General Order 174, *Rules for Electric Utility Substations,* requires each utility to develop and follow an inspection program for its substations, and to update that program as necessary. The General Order requires utilities to follow accepted good practices in the development of these programs, and Commission Decision 12-10-029, which approved the General Order, required the electric utilities to establish these accepted good practices, along with Commission staff, through a series of annual workshops. Finally, General Order 167, E*nforcement of Maintenance and Operations Standards for Generating Facilities*, represents a performance based standard with a set of guidelines.

A potential structure for rules to be considered pursuant to the new requirements in Public Utilities Code Section 364, adopted pursuant to Senate Bill 699, could require each electric utility to use a risk based approach to identify and assess risks to its distribution system, and prepare and follow plans to mitigate those threats. The electric utilities could be allowed to decide to evaluate each asset separately, or develop a tiered system of protection and classify assets within that system. The Commission could also require the electric utilities' plans to meet certain general guidelines (see Section 7.1.1.1 below).

Potentially the Commission could require security plans to be vetted by established security organizations, which could also provide expertise on protection of sensitive information.

A critical portion of a utility's plan would be the development of metrics and consistent testing of the effectiveness of the plan. The Commission has some guidance with respect to metrics in the DHS Chemical Industry Risk Based Performance Standards. However, the electric utilities should propose quantitative metrics for the electric industry. The metrics should include testing and drills, including surprise drills and simulated attacks, to evaluate and monitor the effectiveness of the plans. For such tests, the utilities should utilize outside expertise where necessary.

Under this suggested model, some electric utilities might not need to make changes to their existing physical security measures. For many small distribution substations, typical physical security protections are limited to chain link fences topped by barbed wire, signage, locked gates, appropriate lighting, alarms and access control policies. They may include a camera or simple intrusion control device. For such substations, these security protections may be adequate and the electric utility might not need to upgrade or change them. The proposed model would, however, require the electric utilities to justify their new or existing security measures using a risk based protocol.

Of course, if a thorough risk based analysis identifies any deficiencies in existing physical security measures, the utility must make the appropriate material changes to bring its facilities into compliance.

7.1.1.1 *Guidelines and Industry Standards*

Along with this performance based model, the Commission should adopt at least high level prescriptive guidelines. It is impossible for Commission staff to inspect and evaluate the security needs at the thousands of substations in the state. However, the Commission can adopt guidelines for the development of the plans.

Potential guidelines to consider including along with the risk based process requirements might include:

- *The utility physical security plans should include strict timelines for implementation of the plans.*

- *The utility physical security plan should include consideration of risk and vulnerability to communication facilities necessary for effective operation of alarms and monitoring equipment.*
- *Relevant cybersecurity measures should be designed into the physical security program.*
- *The utility should consider manning or guarding some assets, and provide a clear justification for when such measures are necessary or unnecessary.*
- *The utility should provide a clear justification for perimeter boundaries, such as walls and fences, which includes an analysis of the types of vehicles which might attack and at what speed.*
- *The utility should explain its choice in monitoring and intrusion detection equipment given the location, geography, threat profile, and demographics of the area. The utility should present a plan for consistently inspecting and testing this monitoring equipment under simulated real life events.*
- *The utility should develop preventive maintenance and inspection programs for all physical security related facilities, structures and equipment.*
- *The utility should perform lighting studies at all facilities to determine the optimal lighting system to deter attacks.*
- *The utility should perform a full analysis of vegetation present in the vicinity of the facility and the threat it poses to the physical security.*
- *The utility should consistently test its alarm systems and any alarm interpretation software. It should consistently work to eliminate false alarms.*
- *The utility should look at each asset separately and determine the effect on the grid of the loss of that asset, and the availability of spares and estimated restoration times.*
- *The utility should review its emergency response and preparedness and business continuity planning in conjunction with the development of its physical security plan.*
- *Where appropriate, when developing physical security plans, utilities should consider any special implications related to the protection of modern grid assets including, but not limited to, communication and control devices such as phase*

measurement units, gas insulated substations, inverters, energy storage devices and other distributed generation components.

- *The utility should include physical security equipment, policies and procedures in any corporate quality assurance (QA) and continuous measurable improvement (CMI) programs.*
- *The utility plan should include an effective root cause analysis program for analyzing security failures, including failures during testing and drills.*
- *The utility should look at each piece of equipment in the substation or comprising any other asset separately and determine what the threats to that piece of equipment are, and what vulnerabilities exist. For example,*
  - *What is the most critical piece of equipment in the substation? What is the most vulnerable? The transformers? The batteries? The bushings? The cable terminations? The relay room?*
  - *What are the major modes of attack on those pieces of equipment? Does the mode or method of attack change depending on the season, or the time of day?*
  - *What are the possible modes of protections for those assets and what are the costs? Does the criticality of the piece of equipment justify the mitigation cost?*

The Commission should require that the electric utilities demonstrate they considered cost, environmental impact, existing threat levels, national security information, and other important variables identified in Senate Bill 699 and discussed elsewhere in this whitepaper.

The Commission could also require the electric utilities to follow directives of industry groups such as the Institute of Electrical and Electronics Engineers (IEEE) Substation Physical Security standard, which focuses on theft and vandalism.[78] Both FERC and NERC have developed guidance and best practice documents related to physical security, primarily for the bulk power grid. In 2013 and 2014 FERC staff, along with other energy industry and security agencies, held a series of meetings with utilities and law enforcement to discuss physical security of the grid. In

[78]IEEE Standards Association. 2014. See http://standards.ieee.org/findstds/standard/1402-2000.html

2013 NERC published its latest guidelines on physical security, *Security Guideline for the Electricity Sub-sector: Physical Security Response*.[79]

The Commission could also mandate ongoing workshops to determine accepted good practices in this area, as it did in Decision 12-10-029 adopting General Order 174 for substation inspections. At a later date the Commission may decide to add more specific prescriptive guidelines or requirements (e.g., all facilities of a certain type must utilize a particular deterrent or detection measure). Regardless of whether these new regulations contain requirements for information sharing between utilities, the electric utilities should consider developing a forum for sharing best practices and lessons learned.

If the Commission requires the utilities to develop and submit physical security plans, Commission staff could review the plans and utilize existing industry standards to determine if the plans meet the requirements of Public Utilities Code Section 364 and any implementing Commission decision. Commission staff could physically inspect security measures as part of routine substation or distribution audits, or in new focused security inspections. The Commission might consider contracting with third party security experts in these evaluations or for training of staff to perform these evaluations. In addition, Commission staff may observe drills that the electric utilities conduct to evaluate the effectiveness of the physical security measures adopted.

7.1.2. Protection of Sensitive Information

Given the Freedom of Information Act and the California Public Records Act, along with Commission policies in favor of greater public disclosure,[80] a major concern expressed by the electric utilities during the CPUC June 2014 workshops is the confidentiality of security and business sensitive information. The Commission could limit the information that must be given to the Commission to only the information necessary for the Commission staff to perform their work. Additionally, Senate Bill 699 allows the Commission to redact sensitive security information from public disclosure.

Utilities submit confidential information under the provisions of Public Utilities Code 583 and General Order 66-C, which identify certain information as exempt from public disclosure

[79] Parformak, Paul. op cit, p 17.
[80] See Resolution L-436, *Resolution Regarding the Disclosure of Safety Related Records*, February 14, 2013.

requirements. It is important that all documents receive careful scrutiny before any public release, to avoid disclosing sensitive infrastructure information.

A Commission whitepaper on cybersecurity expressed similar concerns:[81]

> *In order to lower the risks and barriers to sharing information with Commissioners and CPUC Staff, safe harbor provisions may be useful to open up lines of communication between utilities and the CPUC. Safe harbor provisions, coupled with new protections around public disclosure of sensitive data, could result in a beneficial exchange of information and a greater openness between utilities and the CPUC.*

Information regarding distribution assets might be less likely than other system information to fall under the protections of the Protected Critical Information Infrastructure (PCII) program.[82] Regardless, it might be helpful for staff to obtain PCII training and certification.

The Commission might wish to solicit outside organizations, e.g., think-tanks or other governmental agencies, to review the Commission's procedures for handling sensitive information.

8.0 Conclusion

Recent events and increased public awareness directed toward electric grid security, as well as the limited breadth of federal standards, make distribution physical security an important issue at the state level. Recent California state legislation requires the Commission to develop rules for distribution physical security. Given the wide array of threats, equipment designs, and financial abilities within the utility industry, a completely prescriptive regulatory framework is likely not workable. Therefore, the Commission should consider a hybrid risk informed, performance based approach, with high level prescriptive guidelines. Under this model, the electric utilities should develop security plans for their distribution facilities along with metrics to evaluate the effectiveness of those plans. These plans should meet accepted industry best practices. Each electric utility should submit its physical protection plan to the Commission and justify its plan

[81] Malashenko, Villareal and Erikson. Op cit p16.
[82] *Protected Critical Infrastructure Program.* DHS. 2014. See http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program

using a cost-benefit analysis employing risk management techniques. The electric utility should also report annually on its compliance with the Commission's rules, as required by Section 364.

After determining the type of facilities to be covered by the Commission's rules, the Commission should require each utility to:

- *Develop risk based physical security plans for its facilities. Plans should include preventive maintenance programs.*
- *Justify those plans based on current industry best practices and a thorough risk assessment.*
- *Potentially utilize independent third party security experts to prepare and vet the plans.*
- *Present a schedule for implementation of the plans.*
- *Consider multiple alternatives and include metrics for evaluating the efficacy of the plans. The metrics should be quantitative where possible, and the utility should develop tests and drills to stress and evaluate the physical security plan.*
- *Submit the plans for approval by the Commission.*

Appendix A

Senate Bill No. 699

CHAPTER 550

An act to amend Section 364 of the Public Utilities Code, relating to public utilities.

[Approved by Governor September 25, 2014. Filed with Secretary of State September 25, 2014.]

legislative counsel's digest

SB 699, Hill. Public utilities: electrical corporations.

Under existing law, the Public Utilities Commission has regulatory authority over public utilities, including electrical corporations, as defined.

Existing law requires the commission to adopt inspection, maintenance, repair, and replacement standards for the distribution systems of electrical corporations in order to provide high-quality, safe, and reliable service.

Existing law requires the commission to conduct a review to determine whether the standards have been met and to perform the review after every major outage.

This bill would require the commission, in a new proceeding, or new phase of an existing proceeding, to commence on or before July 1, 2015, to consider adopting rules to address physical security risks to the distribution systems of electrical corporations.

Under existing law, a violation of the Public Utilities Act or any order, decision, rule, direction, demand, or requirement of the commission is a crime.

Because the provisions of this bill are within the act and require action by the commission to implement its requirements, a violation of these provisions would impose a state-mandated local program by expanding the definition of a crime.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

The people of the State of California do enact as follows:

SECTION 1. The Legislature finds and declares all of the following:

(a) Physical threats to the electrical distribution system present risks to public health and safety and could disrupt economic activity in California.

(b) Ensuring appropriate actions are taken to protect and secure vulnerable electrical distribution system assets from physical threats that could disrupt

safe and reliable electric service, or disrupt essential public services, including safe drinking water supplies, are in the public interest.

(c) Proper planning, in 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 the potential consequences of such attacks.

SEC. 2. Section 364 of the Public Utilities Code is amended to read:

364. (a) The commission shall adopt inspection, maintenance, repair, and replacement standards, and shall, in a new proceeding, or new phase of an existing proceeding, to commence on or before July 1, 2015, consider adopting rules to address the physical security risks to the distribution systems of electrical corporations. The standards or rules, which shall be prescriptive or performance based, or both, and may be based on risk management, as appropriate, for each substantial type of distribution equipment or facility, shall provide for high-quality, safe, and reliable service.

(b) In setting its standards or rules, the commission shall consider: cost, local geography and weather, applicable codes, potential physical security risks, national electric industry practices, sound engineering judgment, and experience. The commission shall also adopt standards for operation, reliability, and safety during periods of emergency and disaster. The commission shall require each electrical corporation to report annually on its compliance with the standards or rules. Except as provided in subdivision (d), that report shall be made available to the public.

(c) The commission shall conduct a review to determine whether the standards or rules prescribed in this section have been met. If the commission finds that the standards or rules have not been met, the commission may order appropriate sanctions, including penalties in the form of rate reductions or monetary fines. The review shall be performed after every major outage. Any money collected pursuant to this subdivision shall be used to offset funding for the California Alternative Rates for Energy Program.

(d) The commission may, consistent with other provisions of law, withhold from the public information generated or obtained pursuant to this section that it deems would pose a security threat to the public if disclosed.

SEC. 3. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

O

Appendix B

Pacific Gas and Electric Company

Summary Report for Electric Incident Review

Metcalf Substation

As requested by the Safety and Enforcement Division of the California Public Utilities Commission (CPUC), Pacific Gas and Electric Company (PG&E) is providing a root cause analysis about the burglary that occurred at the Metcalf substation in August 2014, including an overview of the actions and enhancements the company has put in place since the initial April 16, 2013, attack on the facility.

Substation physical security is one of the most important issues facing grid operators and PG&E understands how imperative it is to implement strong measures to protect critical substations. PG&E is currently in the first year of a three-year plan to invest more than $100 million to significantly upgrade security at our critical facilities following last year's attack. Major elements of the plan related to physical security were in the process of being implemented at the time of the August burglary. However, some security measures that are part of our plan are still in process and were not in place to help prevent it.

The burglary that occurred at the Metcalf facility in August 2014 underscored the need for additional focus on training and supervision to support the work being done to upgrade technology and physical deterrents at facilities. As a result, PG&E is reprioritizing training and augmenting security supervision to prevent a similar incident.

The root cause analysis contains detailed, confidential information about aspects of the security measures PG&E takes at its facilities and has therefore been sent to the CPUC under confidential protection. Given the appropriate need for the public to have access to information about the two incidents and the steps PG&E is taking to safeguard critical infrastructure, PG&E has developed this public summary report to outline the company's findings.

This summary report includes:

- An overview of the events around the April 16, 2013, Metcalf attack;
- Action steps taken after the April 16, 2013, Metcalf attack;
- An overview of the events around the August 26 - 27, 2014, Metcalf burglary;
- Synopsis of the root cause analysis performed by the company after the August 26 – 27, 2014, Metcalf burglary; and
- Additional action steps taken since the August 26 – 27, 2014, Metcalf burglary.

April 2013 incident at Metcalf Substation and Countermeasures Taken

April 16, 2013, Incident Overview:

On April 16, 2013, gunshots caused extensive damage to the Metcalf Transmission Substation south of San Jose. No one was hurt and no customers lost power as a result of this incident. PG&E's Transmission Control Center operators reacted to alarms and worked to avoid service interruptions for PG&E's customers. Crews also arrived on site to assess the full impact of the damage and begin repairs. PG&E's electric system contains significant redundancies that allow the company to reroute and shift electric load when equipment is damaged. Those redundancies worked as designed.

Following the incident, PG&E worked with federal, state and local agencies, as well as outside consultants to take interim steps to improve substation security while developing a three-year plan to enhance security at critical substations:

- PG&E deployed security guards to provide 24/7 presence at critical substations and increased patrols from local law enforcement;
- PG&E trimmed back vegetation undergrowth around substations to remove potential hiding places; and
- At Metcalf specifically, PG&E installed temporary measures to shield equipment, enhance lighting and obstruct views into the facility while more permanent measures are being designed and engineered.

Additional physical security measures PG&E is currently taking include, among others:

- Opaque or solid walls around the perimeter to shield and obstruct views of equipment inside the substation;
- Enhanced detection and deterrent systems; and
- Improved lighting and camera systems.

PG&E has also worked with law enforcement and industry stakeholders to share information and take appropriate actions on an ongoing basis to protect its facilities.

April 16, 2013, Summary of Actions Taken:

Following the April 2013 attack at the Metcalf substation, PG&E began an assessment and developed a three-year plan to invest more than $100 million to enhance security at its highest priority facilities. Some of the actions taken by PG&E included:

- Worked with local law enforcement to increase security presence at Metcalf and additional facilities (completed within 24 hours of the incident);
- Contracted with a private security company to provide 24/7 security officer coverage (completed within 24 hours of the incident);
- Installed portable lighting (completed within 30 days of the incident);
- Installed temporary fencing (completed within 30 days of the incident);
- Contracted with security consultants to conduct security assessments (completed within 30 days of the incident);
- Completed a series of tours of critical substations with law enforcement agencies. Latitude and longitude coordinates were issued to law enforcement aviation units for aerial patrol when available (June 2013);
- Developed and distributed briefing "tailboards" to employees at major substations to discuss security procedures and suspicious activity reporting (July 2013);
- Received approved permits and removed vegetation surrounding Metcalf (August 2013);
- Initiated an internal training program which included suspicious activity reporting and awareness (September 2013);
- Made improvements to the "Suspicious Activity Reporting" system in Corporate Security (October 2013);
- Participated in an industry and law enforcement sharing campaign in conjunction with the Department of Homeland Security, the Federal Energy Regulatory Commission, North American Electric Reliability Corporation and the Federal Bureau of Investigation. Events were held in each of the 10 Federal Emergency Management Agency jurisdictions (November 2013);
- Initiated an effort to formalize existing policies and procedures associated with the PG&E security system (March 2014);
- Conducted an assessment and test of current security systems at Metcalf (March 2014);
- Enhanced camera surveillance at Metcalf (April 2014);

- Announced a $250,000 reward for information leading to the arrest and conviction of the individual(s) responsible for the attack on the anniversary of the incident (April 2014);
- Worked with local law enforcement to provide enhanced security awareness on the anniversary of the Metcalf event (April 2014);
- Contracted with security consultant to evaluate and provide recommendations for processes and procedures at PG&E's security control center (June 2014);
- Invited Department of Homeland Security to perform a security assessment at Metcalf in coordination with PG&E (June 2014);
- Released a Job Bulletin for additional operators at PG&E's security control center (July 2014);
- Performed on site post order training with security personnel at Metcalf (August 2014);
- Enhanced perimeter lighting at critical locations with additional portable lighting at Metcalf (September 2014);
- Received permit and began construction on a solid wall around Metcalf (September 2014);
- Published Utility Procedure for Security Control Center Alarm Response (September 2014);
- Published Utility Procedure for Security Control Center Incident Response (September 2014); and
- Briefed alarm and incident response protocols and trained security operators on revised response protocols (September 2014).

There were a number of other initiatives that were in the process of being implemented as part of PG&E's security plans when the August 26 – 27, 2014, Metcalf burglary occurred.

August 2014 Burglary at Metcalf Substation, Root Cause and Summary of Actions Taken

Incident Overview

Prior to the August 2014 Metcalf burglary, PG&E's actions to mitigate security threats were mainly focused on upgrading the physical security measures of the company's substations as part of an overall plan to enhance security at substations.

Between the hours of 22:10 on August 26, 2014, and 02:41 on August 27, 2014, PG&E's Metcalf facility was the site of unauthorized entry. As a result of the intrusion, approximately $38,651 of construction tools and equipment was taken.

Despite detection by both the third-party video monitoring system and other security measures, the thefts were not identified until 06:00 hours on August 27, 2014, when construction crews arrived for work.

August 26 – 27, 2014, Summary of Actions Taken

Immediately following the August 2014 burglary, PG&E took numerous initial actions to address security gaps at the facility, including:

- Secured Metcalf Substation fence damaged during the burglary (completed within 24 hours of the incident);
- Checked all equipment within substation for operational damage and found none (completed within 24 hours of the incident);
- Increased security officer presence on site (completed within 24 hours of the incident);
- Enhanced portable lighting onsite (completed within 48 hours of the incident);
- Reinforced and checked to ensure that roving patrols were occurring within Metcalf Substation (completed within 30 days of the incident);
- Re-established onsite roving supervisor position (completed within 30 days of the incident);
- Addressed alarm and incident response protocols for security operations center personnel (completed within 30 days of the incident);
- Performed security review and penetration testing at Metcalf substation (October 2014);
- Enhanced camera systems at Metcalf (October 2014);
- Replaced 3rd party guard contractors (November 2014); and
- Replaced security operations contractors and increased staffing and supervision (November 2014).

Root cause analysis findings

PG&E also assembled an experienced and multi-disciplinary team from across the company to conduct a root cause analysis of the August 2014 incident. The team's root cause analysis, which is submitted in a separate confidential document, found that the security breach was due to the following direct and root causes:

- **Direct Cause:** PG&E's security control center failed to properly respond to alarms and the on-site security officers failed to follow clearly delineated post orders requiring them to perform continuous patrol of Metcalf Substation.

- **Root Cause:** Inadequate training and supervision, created an environment in which PG&E's Security Control Center personnel and on-site security officers failed to follow delineated procedures and post orders.

Additional Actions Planned Based on Root Cause Analysis (Subset of Actions Planned)

As a result of findings outlined in the root cause analysis, PG&E is taking additional actions in a timely manner to prevent a similar incident from occurring. Additional actions include, among other measures:

- Developing and implementing a robust training program for security officers to ensure that alarms are responded to effectively;

- Implementing the use of human performance tools within security control center operations;

- Developing a comprehensive set of security policies and procedures for:
  - Security guards;
  - Work performed at security control center;
  - Training requirements and tracking process for security operators and officers; and
  - Maintenance and repairs for security systems.

Conclusion

PG&E and the utility industry have taken significant steps to increase security following the Metcalf substation attack in April 2013. Although much work had been done to increase physical security at facilities following the incident, the subsequent burglary in August 2014 shows that training and supervision were inadequate to ensure procedures were consistently followed.

PG&E is committed to addressing training and supervision along with other issues raised by the root cause analysis, while continuing to work closely with regulators and law enforcement to maintain the security of the company's facilities.

(End of Appendix B)

Appendix C

(Assembly Bill 1650 adding Public Utilities Code Section 768.6

Assembly Bill No. 1650

CHAPTER 472

An act to add Section 768.6 to the Public Utilities Code, relating to public utilities.

[Approved by Governor September 23, 2012. Filed with Secretary of State September 23, 2012.]

AB 1650, Portantino. Public utilities: emergency and disaster preparedness.

Under existing law, the Public Utilities Commission has regulatory authority over public utilities, including electrical corporations and water corporations, as defined.

Existing law, the California Emergency Services Act, authorizes local governments to create disaster councils by ordinance to develop plans for meeting any condition constituting a local emergency or state of emergency, as specified.

This bill would require the commission to establish standards for disaster and emergency preparedness plans within an existing proceeding, as specified. The bill would require an electrical corporation to develop, adopt, and update an emergency and disaster preparedness plan, as specified. The bill would authorize every city, county, or city and county within the electrical corporation's service area to designate a point of contact for the electrical corporation to consult with on emergency and disaster preparedness plans. The bill would require a water company regulated by the commission to develop, adopt, and update an emergency and disaster preparedness plan, as specified. The bill would find and declare that county and city participation in the preparation of electrical corporations' emergency and

disaster preparedness plans is critical to a statewide emergency response and, thus, is an issue of statewide concern.

The people of the State of California do enact as follows:

SECTION 1. Section 768.6 is added to the Public Utilities Code, to read:

768.6. (a) The commission shall establish standards for disaster and emergency preparedness plans within an existing proceeding, including, but not limited to, use of weather reports to preposition manpower and equipment before anticipated severe weather, methods of improving communications between governmental agencies and the public, and methods of working to control and mitigate an emergency or disaster and its aftereffects. The commission, when establishing standards pursuant to this subdivision, may make requirements for small water corporations similar to those imposed on class A water corporations under paragraph (2) of subdivision (f).

(b) An electrical corporation, as defined in Section 218, providing service in California shall develop, adopt, and update an emergency and disaster preparedness plan in compliance with the standards established by the commission pursuant to subdivision (a).

(1) (A) In developing and adopting an emergency and disaster preparedness plan, an electrical corporation providing service in California shall invite appropriate representatives of every city, county, or city and county within that electrical corporation's service area in California to meet with, and provide consultation to, the electrical corporation.

(B) Every city, county, or city and county within the electrical corporation's service area in California may designate a point of contact for the electrical corporation to consult with on emergency and disaster

preparedness plans.

(C) The electrical corporation shall provide the point of contact designated pursuant to subparagraph (B) with an opportunity to comment on draft emergency and disaster preparedness plans.

(2) For the purposes of best preparing an electrical corporation for future emergencies or disasters, an emergency and disaster preparedness plan shall address recent emergencies and disasters associated with the electrical corporation or similarly situated corporations, and shall address remedial actions for possible emergencies or disasters that may involve that corporation's provision of service.

(3) Every two years, in order to update and improve that electrical corporation's emergency and disaster preparedness plan, an electrical corporation providing service in California shall invite appropriate representatives of every city, county, or city and county within that electrical corporation's service area to meet with, and provide consultation to, the electrical corporation.

(4) For the purposes of best preparing an electrical corporation for future emergencies or disasters, an electrical corporation updating its emergency and disaster preparedness plan shall review the disasters and emergencies that have affected similarly situated corporations since the adoption of the plan, remedial actions taken during those emergencies or disasters, and proposed changes to the plan. The electrical corporation shall adopt in its plan the changes that will best ensure the electrical corporation is reasonably prepared to deal with a disaster or emergency.

(c) A meeting pursuant to subdivision (b) shall be noticed and shall be conducted in a public meeting that allows for the participation of appropriate

representatives of counties and cities within the electrical corporation's service area.

(1) A county participating in a meeting pursuant to subdivision (b) may inform each city within the county of the time and place of the meeting.

(2) An electrical corporation holding a meeting pursuant to subdivision (b) shall provide participating counties and cities with the opportunity to provide written and verbal input regarding the corporation's emergency and disaster preparedness plan. For purposes of this public meeting, an electrical corporation may convene a closed meeting with representatives from every city, county, or city and county within that electrical corporation's service area to discuss sensitive security-related information in the electrical corporation's emergency and disaster preparedness plan and to solicit comment.

(3) An electrical corporation shall notify the commission of the date, time, and location of a meeting pursuant to subdivision (b).

(d) An electrical corporation shall conduct a meeting pursuant to subdivision (b) no later than April 1, 2013, and every two years thereafter.

(e) An electrical corporation shall memorialize a meeting pursuant to subdivision (b), and shall submit its records of the meeting to the commission.

(f) (1) A water company regulated by the commission shall develop, adopt, and update an emergency and disaster preparedness plan in compliance with the standards established by the commission pursuant to subdivision (a). This requirement shall be deemed fulfilled when the water company files an emergency and disaster preparedness plan pursuant to another state statutory requirement.

(2) A water company developing, adopting, or updating an emergency and disaster preparedness plan pursuant to paragraph (1) shall hold meetings with representatives from each city, county, or city and county in the water company's service area regarding the emergency and disaster preparedness plan.

(g) An electrical corporation or a water corporation may fulfill a meeting requirement imposed by this section by making a presentation regarding its emergency and disaster preparedness plan at a regularly scheduled public meeting of each disaster council created pursuant to Article 10 (commencing with Section 8610) of Chapter 7 of Division 1 of Title 2 of the Government Code within the corporation's service area, or at a regularly scheduled public meeting of the governing body of each city, county, or city and county within the service area.

SEC. 2. The Legislature finds and declares that county and city participation in the preparation of electrical corporations' emergency and disaster preparedness plans is critical to a statewide emergency response and, thus, is an issue of statewide concern and not a municipal affair, as that term is used in Section 5 of Article XI of the California Constitution.

(End of Appendix C)

Appendix D

(California Publicly Owned Electric Utilities)

APPENDIX D	
List of California Publicly Owned Electric Utilities	
1.	Alameda Municipal Power P.O. Box H 2000 Grand Street Alameda CA 94501-0263
2.	Anaheim, City of Public Utilities Department Anaheim City Hall West 201 South Anaheim Blvd., Suite 802 Anaheim CA 92805
3.	Azusa Light and Water P.O. Box 9500 729 North Azusa Avenue Azusa CA 91702
4.	Banning, City of Electric Department 176 E. Lincoln Street P.O. Box 998 Banning CA 92220-0998
5.	Biggs Municipal Utilities P.O. Box 307 3016 Sixth Street Biggs CA 95917
6.	Burbank Water and Power 164 West Magnolia Boulevard P.O. Box 631 Burbank CA 91503-0631
7.	Cerritos, City of Cerritos Electric Utility P.O. Box 3130 Cerritos CA 90703
8.	City and County of San Francisco Power Enterprise of the San Francisco Public Utilities Commission 1155 Market Street, 4th Floor San Francisco CA 94103

APPENDIX D	
List of California Publicly Owned Electric Utilities	
9.	City of Industry Administrative Offices 15625 East Stafford Street, Ste. 100 City of Industry CA 91744
10.	Colton Public Utilities 650 N. La Cadena Dr. Colton Ca 92324-2823
11.	Corona, City of Department of Water and Power 755 Corporation Yard Way Corona CA 92880
12.	Eastside Power Authority 14181 Avenue 24 Delano CA 93215
13.	Glendale Water and Power 141 N. Glendale Ave, Level 4 Glendale CA 91206
14.	Gridley Electric Utility 685 Kentucky Street Gridley CA 95948
15.	Healdsburg, City of Electric Department City Hall, 401 Grove Street Healdsburg CA 95448-4723
16.	Imperial Irrigation District 333 E. Barioni Blvd. Imperial CA 92251
17.	Kirkwood Meadows Public Utility District PO BOX 247 Kirkwood CA 95646
18.	Lathrop Irrigation District c/o SSJID PO BOX 747 Ripon, CA 95366

APPENDIX D	
List of California Publicly Owned Electric Utilities	
19.	Lassen Municipal Utility District 65 South Roop Street Susanville CA 96130
20.	Lodi Electric Utility 1331 South Ham Lane Lodi CA 95242-3995
21.	Lompoc, City of P.O. Box 8001 City Hall, 100 Civic Center Plaza Lompoc CA 93438-8001
22.	Los Angeles Department of Water & Power Box 51111 Los Angeles CA 90051-5700
23.	Merced Irrigation District P.O. Box 2288 744 West 20th Street Merced CA 95340
24.	Modesto Irrigation District P.O. Box 4060 Modesto CA 95352-4060
25.	Moreno Valley Electric Utility 14325 Frederick Street, Suite 9 Moreno Valley CA 92553
26.	Needles, City of Public Utility Authority 817 Third Street Needles CA 92363-2933
27.	Palo Alto, City of Utilities Department P.O. Box 10250 Palo Alto CA 94303
28.	Pasadena Water and Power 150 South Los Robles Ave, Suite 200 Pasadena CA 91101-4613

APPENDIX D	
List of California Publicly Owned Electric Utilities	
29.	Pittsburg, City of Pittsburg Power Company d/b/a/ Island Energy 65 Civic Drive Pittsburg CA 94565-3814
30.	Port of Oakland 530 Water Street, Ste. 3 Oakland CA 94607-3814
31.	Port of Stockton P.O. Box 2089 Stockton, CA 95201-2089
32.	Power and Water Resources Pooling Authority 3514 West Lehman Road Tracy CA 95304-9336
33.	Rancho Cucamonga Municipal Utility 10500 Civic Center Drive Rancho Cucamonga CA 91730
34.	Redding Electric Utility P.O. Box 496071 777 Cypress Avenue Redding CA 96049-6071
35.	Riverside, City of Public Utilities Department 3750 University Avenue Riverside CA 92501
36.	Roseville Electric 311 Vernon Street Roseville CA 95678
37.	Sacramento Municipal Utility District P.O. Box 15830 Sacramento CA 95852-1830
38.	Shasta Lake, City of P.O. Box 777 1650 Stanton Drive Shasta Lake CA 96019-0777

APPENDIX D	
List of California Publicly Owned Electric Utilities	
39.	Shelter Cove Resort Improvement District 9126 Shelter Cove Road Whitethorn CA 95589-9079
40.	Silicon Valley Power City of Santa Clara 1601 Civic Center Drive, Suite 202 Santa Clara, California 95050-4109
41.	Trinity Public Utility District P.O. Box 1216 Weaverville CA 96093
42.	Truckee Donner Public Utilities District P.O. Box 309 Truckee CA 96160
43.	Turlock Irrigation District P.O. Box 949 Turlock CA 95381-0949
44.	Ukiah, City of Electric Utilities Division 300 Seminary Avenue Ukiah CA 95482-2680
45.	Vernon, City of Gas & Electric Department 4305 S. Santa Fe Avenue Vernon CA 90058-1714
46.	Victorville Municipal Utilities Services P.O. Box 5001 14343 Civic Drive Victorville CA 92392-5001

(End of Appendix D)

Appendix E

(List of Rural Electric Cooperatives)

APPENDIX E	
List of Rural Electric Cooperatives	
1.	Anza Electric Cooperative, Inc. P.O. Box 391909 58470 Highway 371 Anza CA 92539-1909
2.	Plumas-Sierra Rural Electric Cooperative 73233 State Route 70, Suite A Portola CA 96122-7069
3.	Surprise Valley Electrification Corporation 516 US Hwy. 395E Alturas CA 96101-4228
4.	Valley Electric Association, Inc. 800 E. Highway 372 Pahrump NV 89048-4624

(End of Appendix E)

Appendix F

(Public Owned Utilities Representatives and Agents)

APPENDIX F	
Public Owned Utilities Representatives and Agents	
1.	California Municipal Utilities Association (CMUA) 915 L. Street, Suite 1460 Sacramento, CA 95814
2.	Northern California Power Authority (NCPA) 651 Commerce Drive Roseville, CA 95678
3.	Southern California Public Power Authority 225 South Lake Avenue, Suite 1250 Pasadena, CA 91101

(End of Appendix F)

Appendix G

(List of Facilities Based Communications Carriers

Authorized to Operate in California)

APPENDIX G

List of Facilities-Based Communications Carriers Authorized to Operate in California

Appendix G-1 Local Exchange Carriers	
1	Pacific Bell 525 Market Street, Room 1944 San Francisco CA 94105
2	Verizon California, Inc. 201 Spear Street, 7th Floor San Francisco CA 94105
3	Calaveras Telephone Company PO Box 37 Copperopolis CA 95228
4	Cal-Ore Telephone Company PO Box 847 Dorris CA 96023
5	Ducor Telephone Company PO Box 42230 Bakersfield CA 93384
6	Foresthill Telephone Company, Inc. 811 S. Madera Kerman CA 93630
7	Happy Valley Telephone Co. PO Box 1004 Redmond OR 97756
8	Hornitos Telephone Company PO Box 1004 Redmond OR 97756
9	Kerman Telephone Company 811 South Madera Avenue Kerman CA 93630
10	Pinnacles Telephone Company 340 Live Oak Road Paicines CA 95043
11	The Ponderosa Telephone Company PO Box 21 O'Neals CA 93645

Appendix G-1 Local Exchange Carriers	
12	Surewest Telephone PO Box 969 Roseville CA 95678
13	Sierra Telephone Company, Inc. PO Box 219 Oakhurst CA 93644
14	The Siskiyou Telephone Company PO Box 157 Etna CA 96027
15	Volcano Telephone Company PO Box 1070 Pine Grove CA 95665
16	Winterhaven Telephone Company PO Box 1004 Redmond OR 97756
17	Centurytel of Eastern Oregon, Inc. 6700 Via Austi Parkway Las Vegas NV 89119
18	Citizens Telecommunications Co. of Ca. 9260 E. Stockton Blvd. Elk Grove CA 95624
19	Frontier Communications of the Southwest Inc. 9260 E. Stockton Blvd. Elk Grove CA 95624

Appendix G-2 Competitive Local Carriers	
1.	Pacific Bell 525 Market Street, Room 1944 San Francisco CA 94105
2.	Verizon California, Inc. 201 Spear Street, 7th Floor San Francisco CA 94105
3.	Surewest Telephone PO Box 969 Roseville CA 95678

Appendix G-2 Competitive Local Carriers	
4.	Empire Unified Communications LLC 1 West Main St., Ste. 650 Rochester NY 14614
5.	AT&T Corp. 525 Market Street, Room 1944 San Francisco CA 94105
6.	Sprint Communications Company, LP 201 Mission Street, Suite 1500 San Francisco CA 94105
7.	Fiber Data Systems 203 Bellefontaine Street Pasadena CA 91105
8.	Arrival Communications, Inc. 515 S. Flower Street, 47th Floor Los Angeles CA 90071
9.	MCI Metro Access Transmission Services 201 Spear Street, 7th Floor San Francisco CA 94105
10.	Pac-West Telecomm, Inc. 6500 River Place Blvd. Bldg. 2, Suite 200 Austin TX 78730
11.	CenturyLink Communications, LLC 6700 Via Austi Parkway Las Vegas NV 89119
12.	TW Telecom of California, LP 10475 Park Meadow Drive Littleton CO 80124
13.	Electric Lightwave, Inc. 6160 Golden Hills Dr. Golden Valley MN 55416
14.	IDT America Corp. 520 Broad Street Newark NJ 07102
15.	Frontier Communications of America, Inc. 9260 E. Stockton Blvd. Elk Grove CA 95624
16.	San Carlos Telecom Inc. 2999 Oak Road, Suite 400 Walnut Creek CA 94597

Appendix G-2 Competitive Local Carriers	
17.	Teleport Communications America, LLC 525 Market Street, Room 1944 San Francisco CA 94105
18.	Verizon Select Services, Inc. One Verizon Way, VC53S455 Basking Ridge NJ 07920
19.	Preferred Long Distance, Inc. 16830 Ventura Blvd., Suite 350 Encino CA 91436
20.	Primus Telecommunications, Inc. 7901 Jones Branch Dr., Ste. 900 Mclean VA 22102
21.	The Telephone Connection Local Svcs. 8391 Beverly Blvd., Suite 350 Los Angeles CA 90045
22.	Talk America, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
23.	XO Communications Services 8851 Sandy Parkway Sandy UT 84070
24.	CCT Telecommunications, Inc. 1106 E. Turner Rd., Ste. A Lodi CA 95240
25.	Integrated Telemanagement Services 4100 Guardian Street, Ste. 110 Simi Valley CA 93063
26.	North County Communications Corporation of California 3802 Rosecrans Street, Ste. 485 San Diego CA 92110
27.	Tcast Communications, Inc. 25115 Avenue Stanford, B-210 Valencia CA 91355
28.	Cox California Telcom, LLC 3732 Mt. Diablo Blvd., Suite 358 Lafayette CA 94549
29.	Global Crossing Local Services, Inc. 225 Kenneth Drive Rochester NY 14623

Appendix G-2 Competitive Local Carriers	
30.	Comcast Phone of California, LLC 3055 Comcast Place Livermore CA 94551
31.	McLeod USA Telecommunications Services, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
32.	U.S. Telepacific Corp. 515 S. Flower, 47th Floor Los Angeles CA 90071
33.	Wholesale Airtime, Inc. 27515 Enterprise Circle West Temecula CA 92590
34.	Utility Telephone, Inc. 4202 Coronado Ave. Stockton CA 95204
35.	TGEC Communications Co., LLC 6805 Tujunga Avenue North Hollywood CA 91605
36.	Mpower Communications Corp. 515 S. Flower Street, 47th Floor Los Angeles CA 90071
37.	Access Point, Inc. 1100 Crescent Green Suite 109 Cary NC 27511
38.	Globalinx Enterprises, Inc. 275 Kenneth Drive Rochester NY 14623
39.	Quantumshift Communications, Inc. 12657 Alcosta Blvd., Ste. 418 San Ramon CA 94583
40.	Level 3 Communications, LLC 225 Kenneth Drive Rochester NY 14623
41.	International Telcom, Ltd. 417 Second Avenue West Seattle WA 98119
42.	Incontact, Inc. 7730 S. Union Park Ave., Ste. 500 Midvale UT 84047

Appendix G-2 Competitive Local Carriers	
43.	Peak Communications, Inc. 1442 East Lincoln Ave., Ste. 479 Orange CA 92865
44.	O1 Communications, Inc. 5190 Golden Foothill Parkway El Dorado Hills CA 95762
45.	Point To Point PO Box 3148 Rancho Cordova CA 95741
46.	Integra Telecom 6160 Golden Hills Dr. Golden Valley MN 55416
47.	Southern California Edison 2244 Walnut Grove Ave. Rosemead CA 91770
48.	Paetec Communications, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
49.	Zayo Group, LLC 400 Centennial Parkway, Ste. 200 Louisville CO 80027
50.	Access One, Inc. 820 W. Jackson Blvd., 6th Floor Chicago IL 60607
51.	Navigator Telecommunications, LLC PO Box 13860 North Little Rock AR 72113
52.	Astound Broadband, LLC 401 Kirkland Parkplace, Suite 500 Kirkland WA 98033
53.	Freedom Telecommunications, LLC 624 S. Grand Avenue, Suite 1200 Los Angeles CA 90017
54.	Earthlink Business, LLC 3000 Columbia House Blvd., Suite 106 Vancouver WA 98661
55.	TNCI Operating Company, LLC 114 E. Haley Street, Suite A Santa Barbara CA 93101

Appendix G-2 Competitive Local Carriers	
56.	Unity Telecom, LLC 2997 LBJ Freeway, Suite 225 Dallas TX 75234
57.	Backbone Communications, Inc. 811 Wilshire Blvd., Ste. 1020 Los Angeles CA 90017
58.	Surewest Televideo PO Box 969 Roseville CA 95678
59.	PNG Telecommunications, Inc. 8805 Governors Hill Dr., Suite 250 Cincinnati OH 45249
60.	Acn Communications Services, Inc. 1000 Progress Place Concord NC 28025
61.	AT&T Corp. 525 Market St., Room 1944 San Francisco CA 94105
62.	Reliance Globalcom Services, Inc. 114 Sansome Street, 11th Floor San Francisco CA 94104
63.	IP Networks, Inc. PO Box 192366 San Francisco CA 94119
64.	Broadview Networks, Inc. 1018 West 9th Ave. King Of Prussia PA 19406
65.	Cbeyond Communications, LLC 320 Interstate North Pkwy. SE Atlanta Ga 30339
66.	United States Telesis, Inc. 200 N. Westlake Blvd., Suite 104 Westlake Village CA 91362
67.	Digital Net Phone, LLC 8391 Beverly Blvd., Suite 350 Los Angeles CA 90045
68.	Comtech 21, LLC 1 Barnes Park South Wallingford CT 06492

Appendix G-2 Competitive Local Carriers	
69.	Onvoy, LLC 10300 6th Avenue N. Plymouth MN 55441
70.	RGT Utilities of California, Inc. 1221 Avenue Of The Americas, C2 Level New York NY 10020
71.	Metropolitan Telecomm of Calif., Inc. 44 Wall Street, 14th Floor New York NY 10005
72.	Intrado Communications, Inc. 1601 Dry Creek Drive Longmont CO 80503
73.	Sage Telecom Communications, LLC 10440 North Central Expressway, Suite 700 Dallas TX 75231
74.	Telscape Communications, Inc. 10440 North Central Expressway, Suite 700 Dallas TX 75231
75.	Hypercube Telecom, LLC 3200 W. Pleasant Run Road, Suite 300 Lancaster TX 75146
76.	Call America, Inc. 4202 Coronado Ave. Stockton CA 95204
77.	Curatel, LLC 1605 West Olympic Blvd, Suite 701 Los Angeles CA 90015
78.	Norcast Communications Corporation 1998 Santa Barbara Street, Suite 100 San Luis Obispo CA 93401
79.	BCN Telecom, Inc. 1200 Mt. Kemble Ave., 3rd Floor Harding Township NJ 07960
80.	Wholesale Carrier Services, Inc. 5471 N. University Drive Coral Springs FL 33067
81.	NetFortis Acquisition Co., Inc. 455 Market Street, Suite 620 San Francisco CA 94107

Appendix G-2 Competitive Local Carriers	
82.	Great America Networks, Inc. 10350 Heritage Park, Suite 101 Santa Fe Springs CA 90670
83.	Budget Prepay, Inc. 1325 Barksdale Blvd., Ste. 200 Bossier City LA 71111
84.	Enhanced Communications Network, Inc. 1013 South Glendora Avenue West Covina CA 91790
85.	Creative Interconnect Communications PO Box 656 San Carlos CA 94070
86.	Global Telecom & Technology Americas, Inc. 8484 Westpark Dr., Ste. 720 Mclean VA 22102
87.	McGraw Communications, Inc. 3483 Satellite Blvd., Ste. 202 Duluth GA 30096
88.	Airespring, Inc. 6060 Sepulveda Blvd., Suite 220 Van Nuys CA 91411
89.	Bullseye Telecom, Inc. 25925 Telegraph Road, Suite 210 Southfield MI 48033
90.	Cypress Comms Operating Co., Inc. 75 Erieview Plaza, Suite 400 Cleveland OH 44114
91.	Calltower, Inc. 10701 South River Front Parkway, No. 450 South Jordan UT 84095
92.	Cogent Communications of Calif., Inc. 1015 31st Street, NW Washington DC 20007
93.	DMR Communications, Inc. PO Box 720128 Oklahoma City OK 73172
94.	Telecom North America Inc. 2654 W. Horizon Ridge Pkwy., Ste. B5-143 Henderson NV 89052

Appendix G-2 Competitive Local Carriers	
95.	Teledata Solutions, Inc. 200 N. Westlake Blvd, Suite 104 Westlake Village CA 91362
96.	Crown Castle NG West LLC 2000 Corporate Drive Canonsburg PA 15317
97.	A+ Wireless, Inc. PO Box 5454 Ventura CA 93005
98.	Greenfield Communications, Inc. 34112 Violet Lantern, Ste. C Dana Point CA 92629
99.	Blue Casa Telephone, LLC 10 E. Yanonali Street Santa Barbara CA 93101
100.	Easton Telecom Services, LLC Summit II, Unit A, 3046 Brecksville Rd Richfield OH 44286
101.	Think 12 Corporation 650 East Devon Avenue, Suite 133 Itasca IL 60143
102.	DSCI Corporation C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
103.	First Communications, LLC 3340 West Market Street Akron OH 44333
104.	Granite Telecommunications, LLC 100 Newport Avenue Extension Quincy MA 02171
105.	Paxio, Inc. 2045 Martin Avenue, Suite 204 Santa Clara CA 95050
106.	Advanced Integrated Technologies, Inc. C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
107.	Time Warner Cable Information Services (Calif.) 60 Columbus Circle New York NY 10023

Appendix G-2 Competitive Local Carriers	
108.	TC Telephone, LLC 243 Washington Red Bluff CA 96080
109.	Neutral Tandem California, LLC 550 West Adams Street, Suite 900 Chicago IL 60661
110.	Charter Fiberlink CA-CCO, LLC 12405 Powerscourt Drive St. Louis MO 63131
111.	New Horizons Communications Corporation 420 Bedford St., Suite 250 Lexington MA 02420
112.	Nexus Communications, Inc. 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
113.	Global Connect Telecommunications, Inc. 1146 N. Central Ave., No. 297 Glendale CA 91202
114.	Spectrotel, Inc. C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
115.	Newpath Networks, LLC 2000 Corporate Drive Canonsburg PA 15317
116.	Ca-Clec LLC 2000 Corporate Drive Canonsburg PA 15317
117.	Champion Broadband California, LLC 380 Perry Street Castle Rock CO 80104
118.	Infotelecom, LLC 75 Erieview Plaza, Suite 400 Cleveland OH 44114
119.	Bright House Networks Information Services (Calif.), LLC 4145 S. Falkenburg Road, Suite 7 Riverview FL 33578
120.	Extenet Systems (California) LLC 3030 Warrenville Road, Suite 340 Lisle IL 60532

Appendix G-2 Competitive Local Carriers	
121.	Mpower Networks Services, Inc. 620-630 Third Street San Francisco CA 94107
122.	Ymax Communications Corporation PO Box 6785 West Palm Beach FL 33405
123.	Nextlink Wireless, Inc. 13865 Sunrise Valley Drive Herndon VA 20171
124.	Sunesys, LLC 202 Titus Avenue Warrington PA 18976
125.	Cebridge Telecom Ca, LLC 520 Maryville Center Drive, Suite 300 St. Louis MO 63141
126.	Sonic Telecom, LLC 2260 Apollo Way Santa Rosa CA 95407
127.	MCC Telephony of the West, LLC 100 Crystal Run Road Middletown NY 10941
128.	Cal-Ore Communications, Inc. 719 W. Third Street Dorris CA 96023
129.	Bandwidth.Com Clec, LLC 900 Main Campus Drive, Suite 500 Raleigh NC 27606
130.	Affiniti, LLC 9208 Waterford Center Blvd. Austin TX 78758
131.	Southern California Telephone Company 27515 Enterprise Circle West Temecula CA 92590
132.	Oacys Telecom, Inc. 767 North Porter Road Porterville CA 93257
133.	Conterra Wireless Broadband LLC 2101 Rexford Road, Ste. 200E Charlotte NC 28211

Appendix G-2 Competitive Local Carriers	
134.	Race Telecommunications, Inc. 101 Haskins Way So. San Francisco CA 94080
135.	Wide Voice, LLC 410 South Rampart, Suite 390 Las Vegas NV 89145
136.	Channel Islands Telephone Company 3802 Rosecrans St., Ste. 485 San Diego CA 92110
137.	Rural Broadband Now! LLC 111 South Main Street Willits CA 95490
138.	Telequality Communications, Inc. 24715 Fairway Springs San Antonio TX 78260
139.	Telecommunication Systems, Inc. 275 West St., Ste. 400 Annapolis MD 21401
140.	Telcentris Communications, LLC 9276 Scranton Road, No. 300 San Diego CA 92121
141.	Peerless Network of California, LLC 222 S. Riverside Plaza, Suite 2730 Chicago IL 60606
142.	Raw Bandwidth Telecom, Inc. PO Box 1305 San Bruno CA 94066
143.	Birch Telecom of the West, Inc. 2323 Grand Blvd., Suite 925 Kansas City KS 64108
144.	Shasta County Telecom, Inc. 3802 Rosccrans Street San Diego CA 92110
145.	Convergence Systems, Inc. 10636 Scripps Summit Court, Suite 201 San Diego CA 92131
146.	Empire Unified Communications LLC 1 West Main St., Ste. 650 Rochester NY 14614

Appendix G-2 Competitive Local Carriers	
147.	Public Wireless, Inc. 25 East Trmble Road San Jose CA 95131
148.	Telco Experts, LLC C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
149.	Cruzio Media, Inc. 877 Cedar St., Ste. 150 Santa Cruz CA 95060
150.	Entelegent Solutions, Inc. 3800 Arco Corporate Drive, Ste. 310 Charlotte NC 28273
151.	Mosaic Networx, LLC 454 Las Gallinas Ave., Suite 145 San Rafael CA 94903
152.	Pacific Lightwave, a California Corporation PO Box 10748 Palm Desert CA 92255
153.	Calpop.Com, Inc. 600 West Seventh St., Ste. 360 Los Angeles CA 90017
154.	Broadvox-CLEC, LLC 75 Erieview Plaza, Suite 400 Cleveland OH 44114
155.	Impulse Telecom, LLC 5383 Hollister Ave., Ste. 240 Goleta CA 93111
156.	Blue Rooster Telecom, Inc. PO Box 4959 San Luis Obispo CA 93403
157.	Rosebud Telephone, LLC Box 597 Rosebud TX 76570
158.	Snowcrest Telephone, Inc. 329 A N. Mount Shasta Blvd., Suite 7 Mt. Shasta CA 96067
159.	Airus, Inc. 840 South Canal, 7th Floor Chicago IL 60607

Appendix G-2 Competitive Local Carriers	
160.	Cenic Broadband Initiatives LLC 16700 Valley View Ave., Ste. 400 La Mirada CA 90638
161.	Comity Communications, LLC 3816 Ingersoll Avenue Des Moines IA 50312
162.	Crexendo Business Solutions, Inc. 1615 South 52nd Street Tempe AZ 85044
163.	321 Communications, Inc. PO Box 15857 Brooksville FL 34604
164.	Mobilitie, LLC 660 Newport Center Drive, Suite 200 Newport Beach CA 92660
165.	Big River Telephone Company, LLC 24 S. Minnesota Ave. Cape Girardeau MO 63703
166.	Net Talk.com, Inc. 1100 NW 163rd Drive, Suite B-4 North Miami Beach FL 33169
167.	XYN Communications of California, LLC 8275 S. Eastern Ave., 200 Las Vegas NV 89123
168.	Common Point, LLC 3243 Meadowbrook Springfield IL 62711
169.	Nobelbiz VOIP Services, Inc. 5973 Avenida Encinas, Suite 202 Carlsbad CA 92008
170.	Voxbeam Telecommunications, Inc. 6314 Kingspointe Pkwy., Suite 1 Orlando FL 32819
171.	CVIN, LLC 9479 North Fort Washington, Ste. 105 Fresno CA 93730
172.	Plumas-Sierra Telecommunications 73233 State Route 70, Suite A Portola CA 96122

Appendix G-2 Competitive Local Carriers	
173.	California Broadband Cooperative, Inc. 1101 Nimitz Ave. Vallejo CA 94592
174.	Blue Casa LLC 114 E Haley Street, Suite A Santa Barbara CA 93101
175.	dishNET Wireline L.L.C. 9601 S. Meridian Blvd. Englewood CO 80211
176.	TQAvenger Telecom, LLC 12 Trophy Ridge San Antonio TX 78258
177.	Digital Transportation Corp. 1720 Q Street Sacramento CA 95811
178.	Citrix Communications LLC 1200 18th Street N.W., Suite 1200 Washington DC 20036
179.	Optic Access 533 Airport Blvd., Suite 400 Burlingame CA 94111
180.	Golden Bear Broadband LLC P.O. Box 157 Etna CA 96027
181.	Local Access Services LLC 11442 Lake Butler Blvd. Windermere FL 34786
182.	Vodex Communications Corporation 3185 E2 Airway Avenue Costa Mesa CA 92626
183.	CallFire, Inc. 1410 2nd Street, Floor 2 Santa Monica CA 90401
184.	ATC Outdoor DAS, LLC 10 Presidential Way Woburn Ma 01801
185.	Ultimate Internet Access, Inc. 3633 Inland Empire Blvd., Suite 890 Ontario CA 91764

Appendix G-2 Competitive Local Carriers	
186.	LightSpeed Networks, Inc. 921 SW Washington St., Suite 370 Portland OR 97205

Appendix G-3 Inter-Exchange Carriers	
1.	AT&T Corp. 525 Market Street, Room 1944 San Francisco CA 94105
2.	Global Crossing Telecommunications, Inc. 225 Kenneth Drive Rochester NY 14623
3.	Sprint Communications Company, LP 201 Mission Street, Suite 1500 San Francisco CA 94105
4.	Teleconnect Long Distance Svcs. & Systems 201 Spear Street, 7th Floor San Francisco CA 94105
5.	Fiber Data Systems 203 Bellefontaine Street Pasadena CA 91105
6.	Intellicall Operator Services, Inc. 1049 E Macedonia Church Road Lee FL 32059
7.	Coast International, Inc. 14303 West 95th St. Lenexa KS 66215
8.	Value Added Communications, Inc. 12021 Sunset Hills Road, Suite 100 Reston VA 20190
9.	Matrix Telecom, Inc. 433 E. Las Colinas Blvd., Suite 500 Irving TX 75039
10.	Affinity Network Incorporated 250 Pilot Road, Ste. 300 Las Vegas NV 89119

Appendix G-3 Inter-Exchange Carriers	
11.	Working Assets Funding Service, Inc. 101 Market Street, Suite 700 San Francisco CA 94105
12.	Mitel Netsolutions, Inc. 1146 N. Alma School Rd. Mesa AZ 85201
13.	Ameritel/Amerivision Comms Inc. C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
14.	Arrival Communications, Inc. 515 S. Flower Street, 47th Floor Los Angeles CA 90071
15.	Nos Communications, Inc. 250 Pilot Road, Ste. 300 Las Vegas NV 89119
16.	MCI Metro Access Transmission Services 201 Spear Street, 7th Floor San Francisco CA 94105
17.	Pac-West Telecomm, Inc. 6500 River Place Blvd., Bldg. 2, Suite 200 Austin TX 78730
18.	Norstan Network Services, Inc. 4805 Independence Parkway, Suite 101 Tampa FL 33634
19.	Roudebush Communications 176 W Logan Street, Suite 232 Noblesville IN 46060
20.	Operator Service Company, LLC 6010 Exchange Parkway San Antonio TX 78238
21.	CenturyLink Communications, LLC 6700 Via Austi Parkway Las Vegas NV 89119
22.	National Comtel Network Inc. 21031 Ventura Blvd., Ste. 508 Woodland Hills CA 91364
23.	Buehner-Fry, Inc. C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750

Appendix G-3 Inter-Exchange Carriers	
24.	TW Telecom of California, LP 10475 Park Meadow Drive Littleton CO 80124
25.	Business Discount Plan, Inc. 1 World Trade Center, Suite 800 Long Beach CA 90831
26.	Electric Lightwave Inc. 6160 Golden Hills Dr. Golden Valley MN 55416
27.	MCI Communications Services, Inc. 201 Spear Street, 7th Floor San Francisco CA 94105
28.	Dialink Corporation 1660 S. Amphlett Blvd., Ste. 314 San Mateo CA 94402
29.	Cincinnati Bell Any Distance, Inc. 201 East Fourth Street, 103-1280 Cincinnati OH 45201
30.	TTI National, Inc. 201 Spear Street, 7th Floor San Francisco CA 94105
31.	Covista, Inc. C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
32.	IDT America Corp. 520 Broad Street Newark NJ 07102
33.	Frontier Communications of America, Inc. PO Box 340 Elk Grove CA 95759
34.	Nosva, Limited Partnership 250 Pilot Road, Ste. 300 Las Vegas NV 89119
35.	San Carlos Telecom Inc. 2999 Oak Road, Suite 400 Walnut Creek CA 94597
36.	Teleport Communications America, LLC 525 Market Street, Room 1944 San Francisco CA 94105

Appendix G-3 Inter-Exchange Carriers	
37.	Communications Brokers & Consultants 23939 Ventura Blvd. Calabasas CA 91302
38.	California RSA No. 3 Limited Ptnshp. PO Box 2607 Oakhurst CA 93644
39.	Smart City Networks, LP 28 W. Grand Ave. Montvale NJ 07645
40.	Cybernet Communications Inc. 7750 Gloria Ave. Van Nuys CA 91406
41.	Bulletins, Inc. 39252 Winchester Rd., No. 107-259 Murrieta GA 92563
42.	Verizon Select Services, Inc. One Verizon Way, VC53S455 Basking Ridge NJ 07920
43.	LDC Telecommunications Inc. 2451 McMullen Booth Rd., Ste. 200 Clearwater FL 33759
44.	Tremcom International 6167 Bristol Pkwy., 320 Culver City CA 90230
45.	Preferred Long Distance, Inc. 16830 Ventura Blvd., Suite 350 Encino CA 91436
46.	Primus Telecommunications, Inc. 7901 Jones Branch Dr., Ste. 900 Mclean VA 22102
47.	Worldnet Communications Services, Inc. 80 Wood Rd., Suite 308 Camarillo CA 93010
48.	The Telephone Connection Local Svcs. 8391 Beverly Blvd., Suite 350 Los Angeles CA 90045
49.	Broadwing Communications, LLC 225 Kenneth Drive Rochester NY 14623

Appendix G-3 Inter-Exchange Carriers	
50.	CTC Communications Corp 225 Cedar Hill Street, Suite 111 Marlborough MA 01752
51.	Talk America, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
52.	XO Communications Services 8851 Sandy Parkway Sandy UT 84070
53.	Business Telecom, LLC d/b/a EarthLink Business 2610 Horizon Drive SE, Ste. B Grand Rapids MI 49546
54.	Network Enhanced Technologies, Inc. 700 South Flower Street, Suite 420 Los Angeles CA 90017
55.	CCT Telecommunications, Inc. 1106 E. Turner Road, Ste. A Lodi CA 95240
56.	Integrated Telemanagement Services 4100 Guardian Street, Ste. 110 Simi Valley CA 93063
57.	ABS-CBN Telecom North America, Inc. 150 Shoreline Drive Redwood City CA 94065
58.	North County Communications Corporation of California 3802 Rosecrans, Ste. 485 San Diego CA 92110
59.	Tcast Communications, Inc. 25115 Avenue Stanford Valencia CA 91355
60.	Sierra Telephone Long Distance PO Box 1505 Oakhurst CA 93644
61.	Telecom House Inc. (Sterling) 8421 Wilshire Blvd., Ste. 300 Beverly Hills CA 90211
62.	Global Tel*Link Corporation 12021 Sunset Hills Road, Suite 100 Reston VA 20190

Appendix G-3 Inter-Exchange Carriers	
63.	Cox California Telcom, LLC 3732 Mt. Diablo Blvd., Suite 358 Lafayette CA 94549
64.	Global Crossing Local Services, Inc. 225 Kenneth Drive Rochester NY 14623
65.	Comcast Phone of California, LLC 3055 Comcast Place Livermore CA 94551
66.	BT Americas, Inc. 11440 Commerce Park Drive, Ste. 1000 Reston VA 20191
67.	McLeod USA Telecommunications Services, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
68.	U.S. Telepacific Corp. 515 S. Flower, 47th Floor Los Angeles CA 90071
69.	Verizon Long Distance LLC One Verizon Way, VC53S460 Basking Ridge NJ 07920
70.	Dial Long Distance, Inc. 762 West Ventura Boulevard Camarillo CA 93010
71.	Wholesale Airtime, Inc. 27515 Enterprise Circle West Temecula CA 92590
72.	DeltaCom, LLC 7037 Old Madison Pike, Suite 400 Huntsville AL 35802
73.	Custom Network Solutions, Inc. 210 Route 4 East, Suite 201 Paramus NJ 07652
74.	Legacy Long Distance International, Inc. 10833 Valley View Street, Ste. 150 Cypress CA 90630
75.	Association Administrators, Inc. 180 East Main Street, Ste. 203 Smithtown NY 11787

Appendix G-3 Inter-Exchange Carriers	
76.	Associated Network Partners, Inc. 3243 Meadowbrook Springfield IL 62711
77.	SBC Long Distance, LLC 525 Market St., Room 1944 San Francisco CA 94105
78.	Utility Telephone, Inc. 4202 Coronado Ave. Stockton CA 95204
79.	TGEC Communications Co., LLC 6805 Tujunga Avenue North Hollywood CA 91605
80.	Volcano Long Distance PO Box 1070 Pine Grove CA 95665
81.	Surewest Long Distance PO Box 969 Roseville CA 95678
82.	Net One International, Inc. 457 South Avalon Park Blvd., Suite 500 Orlando FL 32828
83.	Ldmi Telecommunications, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
84.	Mpower Communications Corp. 515 S. Flower Street, 47th Floor Los Angeles CA 90071
85.	Locus Telecommunications, Inc. 2200 Fletcher Ave., 6th Floor Fort Lee NJ 07204
86.	Access Point, Inc. 1100 Crescent Green, Ste. 109 Cary NC 27511
87.	Americatel Corporation 433 E. Las Colinas Blvd., Suite 500 Irving TX 75039
88.	U.S. Telecom Long Distance, Inc. 3960 Howard Hughes Prkwy., Suite 5001F Las Vegas NV 89109

Appendix G-3 Inter-Exchange Carriers	
89.	Globalinx Enterprises, Inc. 275 Kenneth Drive Rochester NY 14623
90.	Quantumshift Communications, Inc. 12657 Alcosta Blvd., Suite 418 San Ramon CA 94583
91.	Level 3 Communications, LLC 225 Kenneth Drive Rochester NY 14623
92.	NTT America, Inc. 757 Third Avenue, Floor 14 New York NY 10017
93.	Infotech Telecomms. and Network Inc. 725 Evans Road San Luis Obisbo CA 93401
94.	Airnex Communications, Inc. 3075 Breckinridge Blvd., Suite 425 Duluth GA 30096
95.	International Telcom, Ltd. 417 Second Avenue West Seattle WA 98119
96.	Network Operator Services, Inc. P.O. Box 3529 Longview TX 75606
97.	Incontact, Inc. 7730 S. Union Park Ave., Ste. 500 Midvale UT 84047
98.	Kddi America, Inc. 825 Third Avenue, 3rd Floor New York NY 10022
99.	American Phone Services, Corp 308 Maxwell Rd, Suite 100 Alpharetta GA 30004
100.	Pacific Centrex Services, Inc. 6805 Tujunga Avenue North Hollywood CA 91605
101.	Peak Communications, Inc. 1442 East Lincoln Avenue, No. 479 Orange CA 92865

Appendix G-3 Inter-Exchange Carriers	
102.	Custom Teleconnect, Inc. 2600 Maitland Center Pky., Suite 300 Maitland FL 32751
103.	CenturyLink Public Communications, Inc. 6700 Via Austi Parkway Las Vegas NV 89119
104.	Clear World Communications Corp. 2901 W. MacArthur Blvd., Suite 204 Santa Ana CA 92704
105.	O1 Communications, Inc. 5190 Golden Foothill Parkway El Dorado Hills CA 95762
106.	Point To Point, Inc. PO Box 3148 Rancho Cordova CA 95741
107.	Advanced Telcom, Inc. 6160 Golden Hills Dr. Golden Valley MN 55416
108.	Southern California Edison 2244 Walnut Grove Ave. Rosemead CA 91770
109.	Paetec Communications, Inc. 655 W. Broadway, Ste. 850 San Diego CA 92101
110.	Zayo Group, LLC 400 Centennial Parkway, Suite 200 Louisville CO 80027
111.	Wiltel Communications, LLC 225 Kenneth Drive Rochester NY 14623
112.	Advantage Telecommunications Corp C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
113.	Astound Broadband, LLC 401 Kirkland Parkplace, Suite 500 Kirkland WA 98033
114.	Freedom Telecommunications, LLC 624 S. Grand Avenue, Suite 1200 Los Angeles CA 90017

Appendix G-3 Inter-Exchange Carriers	
115.	Earthlink Business, LLC 3000 Columbia House Blvd., Suite 106 Vancouver WA 98661
116.	Unity Telecom, LLC 2997 LBJ Freeway, Suite 225 Dallas TX 75234
117.	Openpop.Com, Inc. 3055 Wilshire Blvd., Suite 730 Los Angeles CA 90010
118.	Backbone Communications, Inc. 811 Wilshire Blvd., Ste. 1020 Los Angeles CA 90017
119.	Surewest Televideo PO Box 969 Roseville CA 95678
120.	Network IP, LLC 1807 Judson Road Longview TX 75605
121.	PNG Telecommunications, Inc. 8805 Governors Hill Dr., Suite 250 Cincinnati OH 45249
122.	AT&T Corp. 525 Market St., Room 1944 San Francisco CA 94105
123.	Reliance Globalcomm Services, Inc. 114 Sansome Street, 11th Floor San Francisco CA 94104
124.	IP Networks, Inc. PO Box 192366 San Francisco CA 94119
125.	Broadview Networks, Inc. 1018 West 9th Ave. King Of Prussia PA 19406
126.	Telmex USA, LLC 3350 SW 148 Avenue, Suite 400 Miramar FL 33027
127.	ANPI Business, LLC 7460 Warren Parkway, Ste. 218 Frisco TX 75034

Appendix G-3 Inter-Exchange Carriers	
128.	Cbeyond Communications, LLC 320 Interstate North Pkwy. SE Atlanta GA 30339
129.	Digital Net Phone, LLC 8391 Beverly Blvd., Suite 350 Los Angeles CA 90045
130.	Encompass Communications, LLC 119 West Tyler Street, Suite 260 Longview TX 75601
131.	Onvoy, LLC 10300 6th Avenue N. Plymouth MN 55441
132.	RGT Utilities of California, Inc. 1221 Avenue Of The Americas, C2 Level New York NY 10020
133.	Aries Network, Inc. 5973 Avenida Encinas, Suite 202 Carlsbad CA 92008
134.	Intrado Communications, Inc. 1601 Dry Creek Drive Longmont CO 80503
135.	Sage Telecom Communications, LLC 10440 North Central Expressway, Suite 700 Dallas TX 75231
136.	Telscape Communications, Inc. 10440 North Central Expressway, Suite 700 Dallas TX 75231
137.	Call America, Inc. 4202 Coronado Ave. Stockton CA 95204
138.	Curatel, LLC 1605 West Olympic Blvd., Suite 701 Los Angeles CA 90015
139.	Norcast Communications Corporation 1998 Santa Barbara Street, Suite 100 San Luis Obispo CA 93401
140.	Wholesale Carrier Services, Inc. 5471 N. University Drive Coral Springs FL 33067

Appendix G-3 Inter-Exchange Carriers	
141.	NetFortis Acquisition Co., Inc. 455 Market Street, Suite 620 San Francisco CA 94107
142.	Great America Networks, Inc. 10350 Heritage Park, Suite 101 Santa Fe Springs CA 90670
143.	Budget Prepay, Inc. 1325 Barksdale Blvd., Ste. 200 Bossier City LA 71111
144.	Creative Interconnect Communications PO Box 656 San Carlos CA 94070
145.	Onelink Communications, Inc. 8400 N. University Drive, Suite 204 Tamarac FL 33321
146.	New World Telecom International, Inc. 2711 Centerville Road, Suite 400 Wilmington DE 19808
147.	McGraw Communications, Inc. 3483 Satellite Blvd., Ste. 202 Duluth GA 30096
148.	Cypress Comms. Operating Co., Inc. 75 Erieview Plaza, Suite 400 Cleveland OH 44114
149.	Calltower, Inc. 10701 South River Front Parkway, No. 450 South Jordan UT 84095
150.	Cogent Communications of Calif., Inc. 1015 31st Street, NW Washington DC 20007
151.	DMR Communications, Inc. PO Box 720128 Oklahoma City OK 73172
152.	Telecom North America Inc. 2654 W. Horizon Ridge Pkwy., Ste. B5-143 Henderson NV 89052
153.	Broadband Dynamics, LLC 8757 E. Via De Commercio Scottsdale AZ 85258

Appendix G-3 Inter-Exchange Carriers	
154.	Crown Castle NG West LLC 2000 Corporate Drive Canonsburg PA 15317
155.	A+ Wireless, Inc. PO Box 5454 Ventura CA 93005
156.	Blue Casa Telephone, LLC 10 E. Yanonali Street Santa Barbara CA 93101
157.	Chunghwa Telecom Global, Inc. 2107 N. First St., Ste. 580 San Jose CA 95131
158.	Independent Telecommunications Systems, 4079 Park East Court Kentwood MI 49546
159.	Granite Telecommunications, LLC 100 Newport Avenue Extension Quincy MA 02171
160.	Paxio, Inc. 2045 Martin Avenue, Suite 204 Santa Clara CA 95050
161.	Advanced Integrated Technologies, Inc. C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
162.	Time Warner Cable Information Services 60 Columbus Circle New York NY 10023
163.	TC Telephone, LLC 243 Washington Red Bluff CA 96080
164.	Neutral Tandem California, LLC 550 West Adams Street, Suite 900 Chicago IL 60661
165.	Charter Fiberlink CA-CCO, LLC 12405 Powerscourt Drive St. Louis MO 63131
166.	Lucky Communications, Inc. 1028 Mission Street San Francisco CA 94103

Appendix G-3 Inter-Exchange Carriers	
167.	Globalphone Corporation 137 North Washington Street, Suite 200 Falls Church VA 22046
168.	Worldwide Telecommunications, Inc. 4505 Las Virgenes Road, Suite 115 Calabasas CA 91302
169.	Global Connect Telecommunications, Inc. 1146 N. Central Ave., No. 297 Glendale CA 91202
170.	Newpath Networks, LLC 2000 Corporate Drive Canonsburg PA 15317
171.	Ca-Clec LLC 2000 Corporate Drive Canonsburg PA 15317
172.	Champion Broadband California, LLC 380 Perry Street Castle Rock CO 80104
173.	Infotelecom, LLC 75 Erieview Plaza, Suite 400 Cleveland OH 44114
174.	Bright House Networks Information Services (Calif.), LLC 4145 S. Falkenburg Road, Suite 7 Riverview FL 33578
175.	Extenet Systems (California) LLC 3030 Warrenville Road, Suite 340 Lisle IL 60532
176.	IBFA Acquisition Company, LLC C/O CSI, 740 FL. Central Parkway, Ste. 2028 Longwood FL 32750
177.	800 Response Information Services, LLC 1795 Williston Road, Suite 200 South Burlington VT 05403
178.	Mpower Networks Services, Inc. 620-630 Third Street San Francisco CA 94107
179.	Nextlink Wireless, Inc. 13865 Sunrise Valley Drive Herndon VA 20171

Appendix G-3 Inter-Exchange Carriers	
180.	Sunesys, LLC 202 Titus Avenue Warrington PA 18976
181.	Cebridge Telecom Ca, LLC 520 Maryville Center Drive, Suite 300 St. Louis MO 63141
182.	Sonic Telecom, LLC 2260 Apollo Way Santa Rosa CA 94507
183.	Smart Choice Communications, LLC PO Box 720128 Oklahoma City OK 73172
184.	MCC Telephony of the West, LLC 100 Crystal Run Road Middletown NY 10941
185.	BLC Management LLC 6905 N. Wickham Road, Suite 403 Melbourne FL 32940
186.	Alliance Group Services, Inc. 1221 Post Road East Westport CT 06880
187.	Bandwidth.Com Clec, LLC 900 Main Campus Drive, Suite 500 Raleigh NC 27606
188.	Oacys Telecom, Inc. 767 North Porter Road Porterville CA 93257
189.	Channel Islands Telephone Company 3802 Rosecrans St., Ste. 485 San Diego CA 92110
190.	Telequality Communications, Inc. 24715 Fairway Springs San Antonio TX 78260
191.	CapTex Telecom, LLC 119 West Tyler Street, Ste. 100 Longview TX 75601
192.	Telcentris Communications, LLC 9276 Scranton Road, No. 300 San Diego CA 92121

Appendix G-3 Inter-Exchange Carriers	
193.	Roadway Communications, Inc. 16012 S. Western Avenue, Suite 303 Gardena CA 90247
194.	Ekit.Com Inc. 27 Drydock Ave., 5th Floor Boston MA 02210
195.	Call One Inc. 225 W. Wacker Drive, 8th Floor Chicago IL 60606
196.	Momentum Telecom, Inc. 880 Montclair Road, Suite 400 Birmingham AL 35213
197.	Peerless Network of California, LLC 222 S Riverside Plaza, Suite 2730 Chicago IL 60606
198.	Shasta County Telecom, Inc. 3802 Rosccrans Street San Diego CA 92110
199.	Convergence Systems, Inc. 10636 Scripps Summit Court, Suite 201 San Diego CA 92131
200.	Callcatchers, Inc. 169 Saxony Rd., Ste. 206 Encinitas CA 92024
201.	Public Wireless, Inc. 25 East Trimble Road San Jose CA 95131
202.	X2 Telecom, LLC PO Box 90346 Santa Barbara CA 93190
203.	Cruzio Media, Inc. 877 Cedar St., Ste. 150 Santa Cruz CA 95060
204.	Mosaic Networx, LLC 454 Las Gallinas Ave., Suite 145 San Rafael CA 94903
205.	Broadvox-CLEC, LLC 75 Erieview Plaza, Suite 400 Cleveland OH 44114

Appendix G-3 Inter-Exchange Carriers	
206.	Impulse Telecom, LLC 5383 Hollister Ave., Ste. 240 Goleta CA 93111
207.	Telus Communications Company 500 8th Street, NW Washington DC 20004
208.	Frontier Communications Online & LD 9260 E. Stockton Blvd. Elk Grove CA 95624
209.	Blue Rooster Telecom, Inc. PO Box 4959 San Luis Obispo CA 93403
210.	Rosebud Telephone, LLC PO Box 597 Rosebud TX 76570
211.	Pay Tel Communications, Inc. P.O. Box 8179 Greensboro NC 27419
212.	Airus, Inc. 840 South Canal, 7th Floor Chicago IL 60607
213.	Cenic Broadband Initiatives LLC 1415 L Street, Suite 870 Sacramento CA 95814
214.	Comity Communications, LLC 3816 Ingersoll Avenue Des Moines IA 50312
215.	Digital West Networks, Inc. 3620 Sacramento Drive, Suite 102 San Luis Obispo CA 93401
216.	Splice Communications, Inc. 1900 S. Norfolk St., Suite 350 San Mateo CA 94403
217.	Bestel (USA), Inc. 2323 Bryan Street, Suite 2040 Dallas TX 78205
218.	Crexendo Business Solutions, Inc. 1615 South 52nd Street Tempe AZ 85281

Appendix G-3 Inter-Exchange Carriers	
219.	Mobilitie, LLC 660 Newport Center Drive, Suite 200 Newport Beach CA 92660
220.	Big River Telephone Company, LLC 24 S. Minnesota Ave. Cape Girardeau MO 63703
221.	XYN Communications of California, LLC 8275 S. Eastern Ave., 200 Las Vegas NV 89123
222.	Common Point, LLC 3243 Meadowbrook Springfield IL 62711
223.	Voxbeam Telecommunications, Inc. 6314 Kingspointe Pkwy., Suite 1 Orlando FL 32819
224.	Plumas Sierra Telecommunications 73233 State Route 70, Suite A Portola CA 96122
225.	California Broadband Cooperative, Inc. 1101 Nimitz Ave. Vallejo CA 94592
226.	Masergy Communications, Inc. 2740 North Dallas Parkway Plano TX 75093
227.	Lit San Leandro, LLC 777 Davis Street San Leandro CA 94577
228.	IFN.com, Inc. 9841 Airport Blvd., 9th Floor Los Angeles CA 90045
229.	LCB Communications, LLC P.O. Box 1246 Sam Martin CA 95020
230.	Telecircuit Network Corporation 1725 Winward Concourse, Suite 150 Alpharetta GA 30005
231.	Optic Access 533 Airport Blvd., Suite 400 Burlingame CA 94111

Appendix G-3 Inter-Exchange Carriers	
232.	Metro Star Networks, Inc. 145 S. Halcyon Rd., Suite E Arroyo Grande CA 93420
233.	Local Access Services LLC 11442 Lake Butler Blvd. Windermere FL 34786
234.	Public Interest Telecom of CA 1050 Heinz Ave. Berkeley CA 94710
235.	Vodex Communications Corporation 3185 E2 Airway Avenue Costa Mesa CA 92626
236.	Transbeam, Inc. 8 West 38th St., 7th Floor New York City NY 10018
237.	Global Telco Group Inc. 1420 Spring Hill Road, Suite 401 Mclean VA 22102
238.	Sage Communications, Inc. 4274 Enfield Court, Suite 1600 Palm Harbor FL 34685
239.	CallFire, Inc. 1410 2nd Street, Floor 2 Santa Monica CA 90401
240.	Smart Card Services, Inc. 15953 NW 16th Street Pembroke Pines FL 33028
241.	Surfnet Communications, Inc. 25600 Hillside Road Los Gatos CA 95033
242.	Viasat Inc. 349 Inverness Drive South Englewood CO 80112
243.	Ultimate Internet Access, Inc. 3633 Inland Empire Blvd., Suite 890 Ontario CA 91764

Appendix G-3 Inter-Exchange Carriers	
244.	LightSpeed Networks, Inc. 921 SW Washington St., Suite 370 Portland OR 97205

Appendix G-4 Commercial Mobile Radio Service Providers (Cellular Carriers)	
1.	Cellco Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
2.	GTE Mobilnet of CA., Ltd. Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
3.	Los Angeles SMSA Limited Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
4.	Sacramento Valley Ltd. Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
5.	Fresno MSA Ltd. Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
6.	GTE Mobilnet of Santa Barbara 201 Spear Street, 7th Floor San Francisco CA 94105
7.	Santa Barbara Cellular Systems, Ltd. 1525 Market St., Room 1944 San Francisco CA 94105
8.	AT&T Mobility Wireless Operations Holdings Inc. 525 Market St. San Francisco CA 94105
9.	WWC License, LLC 180 Washington Valley Road Bedminster NJ 07921
10.	California RSA No. 3 Ltd. Partnership PO Box 2607 Oakhurst CA 93644

Appendix G-4 Commercial Mobile Radio Service Providers (Cellular Carriers)	
11.	Verizon Wireless, LLC 201 Spear Street, 7th Floor San Francisco CA 94105
12.	Modoc RSA Limited Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
13.	California RSA No. 4 Ltd. Partnership 201 Spear Street, 7th Floor San Francisco CA 94105
14.	United States Cellular Corporation 8410 West Bryn Mawr Chicago IL 60631
15.	T-Mobile West LLC 1755 Creekside Oasks Dr., STE. 190 Sacramento CA 95833
16.	New Cingular Wireless PCS, LLC 525 Market St., Room 1944 San Francisco CA 94105
17.	Cricket Communications, Inc. 525 Market St., Room 1944 San Francisco CA 94105
18.	Metropcs California, LLC 1755 Creekside Oasks Dr., Ste. 190 Sacramento CA 95833
19.	Accessible Wireless, LLC 100 Via Dela Valle, Suite 200 Del Mar CA 92014
20.	California Valley Broadband, LLC 1015 - B Airport Road Rio Vista CA 94571

Appendix G-5 Radio Telephone Utilities	
1.	Madera Radio Dispatch PO Box 28 Madera CA 93639-0028
2.	Fresno Mobile Radio Inc. 160 North Broadway Fresno CA 93701
3.	American Messaging Services, LLC 1720 Lakepointe Dr., Ste. 100 Lewisville TX 75057
4.	Velocita Wireless 70 Wood Avenue South, 3rd Floor Iselin NJ 08830
5.	USA Mobility Wireless, Inc. 6850 Versar Center, Suite 420 – Tax Dept. Springfield VA 22151
6.	Telefonica USA, Inc. 1111 Brickell Avenue, 10th Floor Miami FL 33131

(End of Appendix G)

Appendix H

(Service List of Resolution No. W-4823)

Service List of Resolution No. W-4823

Edward Jackson
Park Water Company
P. O. Box 7002
DOWNEY CA 90241-7002

Leigh K. Jordan
Apple Valley Ranchos Wtr. Co.
P. O. Box 7002
DOWNEY CA 90241

Lawrence Morales
East Pasadena Water Co.
3725 East Mountain View Ave.
PASADENA CA 91107

Robert J. DiPrimio
Valencia Water Co.
24631 Avenue Rockefeller
VALENCIA CA 91335

Robert L. Kelly
Suburban Water Systems
1211 E. Center Court Drive
COVINA CA 91724-3603

Daniel A. Dell'Osa
San Gabriel Valley Water Co.
P.O. Box 6010
EL MONTE CA 91734

Michael Whitehead
San Gabriel Valley Water Co.
P. O. Box 6010
EL MONTE CA 91734

Timothy J. Ryan, Gen. Counsel
San Gabriel Valley Water Co.
P. O. Box 6010
EL MONTE CA 91734

Keith Switzer
Golden State Water Company
630 East Foothill Blvd.
SAN DIMAS CA 91773-9016

Robert Thomas Adcock
Alco Water Service
249 Williams Road
SALINAS CA 93905

Martin A. Mattes
California Water Association
50 California Street
SAN FRANCISCO CA 94111

Francis S. Ferraro
California Water Service Co.
1720 N. First Street
SAN JOSE CA 95112-4598

John Roeder
Great Oaks Water Company
P. O. Box 23490
SAN JOSE CA 95153-3490

Palle Jensen
San Jose Water Company
374 W. Santa Clara Street
SAN JOSE CA 95196-0001

Robert C. Cook, Sr.
Fruitridge Vista Water Company
1108 Second Street, Suite 204
SACRAMENTO CA 95814

David P. Stephenson
California-American Water Co.
4701 Beloit Drive
SACRAMENTO CA 95838

Robert S. Fortino
Del Oro Water Company, Inc.
Drawer 5172
CHICO CA 95927

John Garon
Golden State Water Company
630 East Foothill Blvd.
SAN DIMAS CA 91773-9016

Gladys Rosendo
Golden State Water Company
630 East Foothill Blvd.
SAN DIMAS CA 91773-9016

John K. Hawks
California Water Association
Mail Code E3-608
601 Van Ness Ave., 2047
SAN FRANCISCO CA 94102

E. Garth Black
Cooper, White, & Cooper, LLP
201 California Street, 17th Street
SAN FRANCISCO CA 94111

Sarah Leeper
Attorney at Law
Manatt, Phelps & Phillips, LLP
One Embarcadero Ctr., 30th Floor
SAN FRANCISCO A 94111

Jose E. Guzman, Jr.
California Water Association
50 California Street
SAN FRANCISCO CA 94111

Joseph M. Karp
Winston & Strawn, LLP
101 California St., 39th Floor
SAN FRANCISCO CA 94111

Thomas Smegal
California Water Service Company
1720 North First
SAN JOSE CA 95112

Edward Howard
CPUC – Policy & Planning Div.
505 Van Ness Avenue, Rm. 5119
SAN FRANCISCO CA 94102

Jacquline A. Reed
CPUC – ALJ
505 Van Ness Avenue, Rm. 5017
SAN FRANCISCO CA 94102

Jason J. Zeller
CPUC-Legal Division, Rm. 5105
505 Van Ness Avenue
SAN FRANCISCO CA 94102

Joe Como
CPUC – DRA- Admin. Branch
505 Van Ness Avenue, Rm. 4101
SAN FRANCISCO CA 94102

Ravi Kumra
CPUC – DWA
505 Van Ness Avenue
SAN FRANCISCO CA 94102

Ting-Pong Yuen
CPUC – ORA 3-D
505 Van Ness Avenue
SAN FRANCISCO CA 94102

Yoke W. Chan
CPUC – ORA 3-D
505 Van Ness Avenue
SAN FRANCISCO CA 94102

(End of Appendix H)