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 324 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

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.

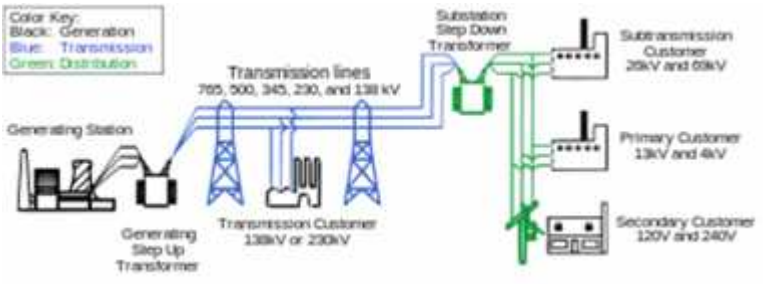
This whitepaper discusses the relevant issues in physical security for the electric distribution system, with a particular focus on advising policymakers on implementation scenarios for the new requirements codified in Section 364 of the Public Utilities Code, as amended by Senate Bill 699.[5] Section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

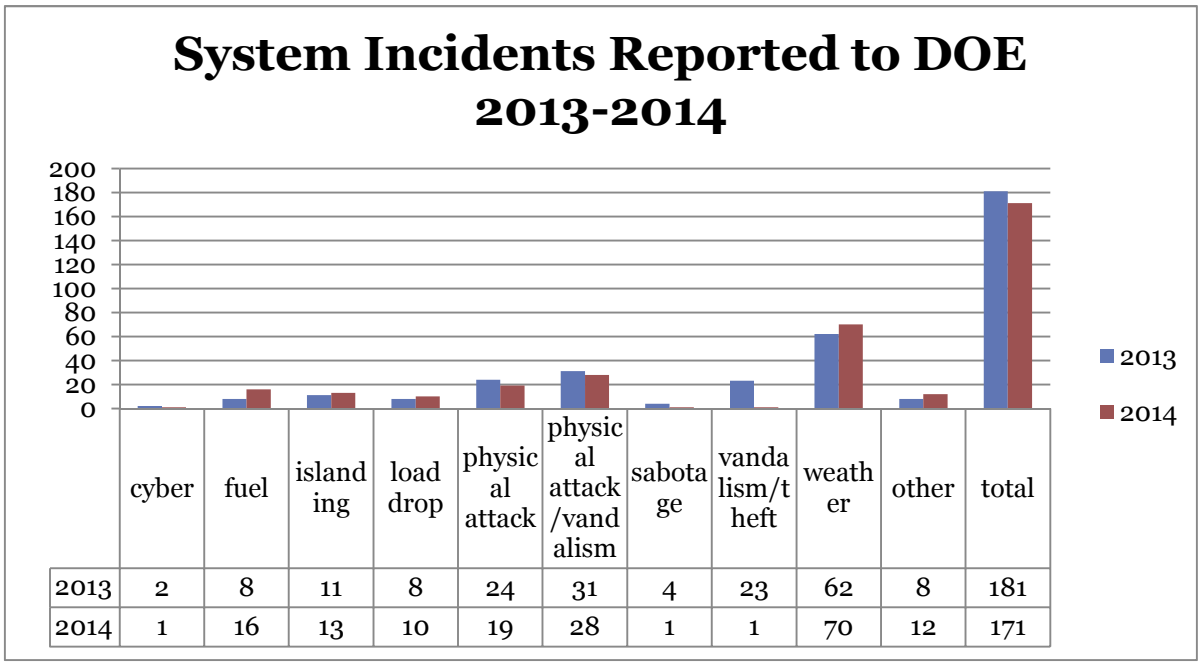
The major risks associated with a physical attack against electricity grid facilities are incidents that cause substantial enough damage, and result in widespread outages that last for days or weeks as critical equipment is repaired or replaced. While there have been many examples of extreme weather 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-201412288472878548O.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]

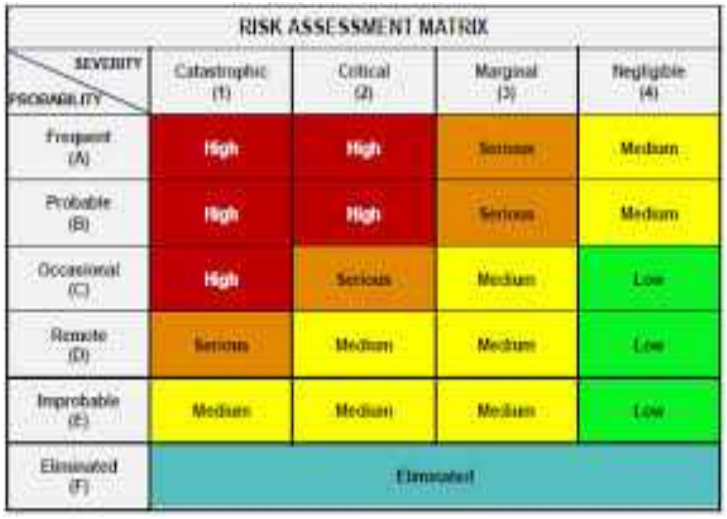
In the electric industry, threats can be classified by the source and the methodology. As to the source of physical risks and threats, they can potentially emanate from vandals or thieves, disgruntled employees and possibly terrorist entities. The methodology of attack can include vehicle (land or aerial) 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 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.[81]

A Commission whitepaper on cybersecurity expressed similar concerns:[82]

> *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.[83] 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

[82] Malashenko, Villareal and Erikson. Op cit p16.
[83] *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.