# Safety and Enforcement Division

## Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699

## A CPUC Staff White Paper

## January 2018


California Public Utilities Commission
Safety and Enforcement Division
Risk Assessment and Safety Advisory Section

Jeremy Battis
Martin Kurtovich, PE
Arthur O'Donnell

## ACKNOWLEDGMENTS

SED staff would like to thank the many interested and engaged stakeholders who contributed to the physical security proceeding and the public participation process. These parties include the California Office of Emergency Services (Cal-OES), such Federal agencies as the Department of Homeland Security (DHS), the North American Electric Reliability Corporation (NERC), and the Federal Bureau of Investigation (FBI).

This work benefitted greatly from input by members of a technical working group that involved the investor- and publicly-owned electric utilities. Valuable information also came from trade associations, including the Edison Electric Institute (EEI), the National Rural Electric Cooperative Association (NRECA), the California Municipal Utilities Association (CMUA), and the Northern California Power Agency (NCPA), as well as electric professional societies which include the Institute for Electric and Electronic Engineers (IEEE).

Deserving special mention and thanks is the audit and compliance staff at the Western Electricity Coordinating Council (WECC), who – as enforcement regulators for transmission assets under NERC CIP -- on several occasions shared expertise with SED staff. From these interviews, SED staff knowledge and understanding benefitted from WECC's deep experience with the validation and implementation of electric utilities' physical security plans. WECC staff's verification of assumptions and service as a sounding board for ideas was invaluable as California sought to apply security requirements to its distribution assets.

# CONTENTS

# 1 EXECUTIVE SUMMARY

The April 2013 sniper attack on Pacific Gas and Electric's Metcalf substation has been described variously as a "wake-up call" or an alarm for the electric utility industry to apply closer scrutiny to the vulnerability of key infrastructure to various kinds of attack – whether physical, as in the Metcalf shooting, or in the form of cyber attacks that might impair physical operations.

For the electric grid, this has led to calls to guard against potential attacks on not only high-profile, Federally-regulated assets, but also facilities traditionally left to state-level purview, such as distribution assets. Efforts to ensure the security of key generating facilities along with critical infrastructure at the high-voltage transmission level have been ongoing for about the past 15 years, there is a lingering concern that the distribution grid might also be vulnerable to physical attack.

Following the Metcalf incident, California lawmakers passed new legislation, SB 699[1] (Hill, 2014), that directed the California Public Utilities Commission to explore policies and practices related to physical security of electric distribution assets. Specifically, the law directed the Commission to consider adoption of new standards and rules to address any physical security risk to the distribution system of California's electric corporations so as to ensure "high-quality, safe, and reliable service."

This Staff White Paper report provides background material developed in support of the CPUC's response to SB 699, carried out within the Rulemaking proceeding R.15-06-009.[2] CPUC staff at the Safety and Enforcement Division's Risk Assessment and Safety Advisory section conducted a series of workshops to gather expert opinion and aid understanding of security practices in place at the federal level. This public engagement effort informed the proceeding about potential practices and policies that might apply to state-jurisdictional entities.

[1] Public Utilities Code Section 364 *(Amended by Stats. 2015, Ch. 612, Sec. 10. Effective January 1, 2016)*. Available for download at: http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB699

[2] CPUC, Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electric Corporations, June 2015.
Available for download at docs.cpuc.ca.gov/PublishedDocs/Efile/G000/M173/K203/173203646.PDF

The three major issue areas addressed in this proceeding are 1) identifying a process for the prioritization of strategic electrical facilities and determining appropriate security measures or approaches to ensuring resiliency of the system, 2) establishing practices for the exchange of highly-confidential or "sensitive" information between utilities and the Commission, and 3) confirming whether existing incident reporting requirements are adequate. These three subject areas are examined with an eye toward ensuring appropriate regulatory oversight of jurisdictional utility operational performance, and providing a mechanism for entities not subject to CPUC ratemaking authority to identify their own most appropriate measures.

With the experience electric utilities have gained in complying with relatively new Federal standards for critical infrastructure protection, California's electric system operators have already identified the most critical assets subject to potential attack, and have taken steps to increase security via "hardening" of select critical infrastructure, especially substation facilities, as well as additional security measures, such as video surveillance, alarms and patrols. Already, California's jurisdictional utilities (aka Investor Owned Utilities or "IOUs") have sought approval for tens of millions of dollars in General Rate Case funding to ensure physical security.

On the issue of physical security, it has become clear that there exists a clear distinction between those issues that apply to distribution assets versus more critical assets on the high-voltage transmission networks. Even a coordinated attack against distribution facilities is unlikely to result in widespread system disturbances or cascading outages, owing to the local grid's built-in redundancy and the relatively small service share typically assigned to any single distribution substation. Depending on the design of the distribution system, redundancy can be built into system such that disruptions can be limited and an affected distribution circuit can be served by an alternative substation.

Reasonable security measures for utility distribution assets are not predicated on how well defended these assets may be. Rather, there should be a balance between preventive measures addressing infrastructure and security improvements, and ensuring the resiliency of the distribution network. Thus, effective risk mitigation could be made to address both the likelihood of an adverse event, *and* reduce the potential consequences of an incident.

Additionally, despite an emphasis on averting planned physical attacks, such as the Metcalf shooting, the vast majority of so-called physical security incidents on the distribution system have consisted of minor property crimes such as vandalism, copper theft, and trespassing. These crimes are generally committed not by determined or organized attackers, but by opportunists. Appreciating this distinction will lead to more effective approaches at a more reasonable cost than would a "one size fits all" strategy of attempting to "harden" all facilities as if they were critical assets.

Eventually, for CPUC jurisdictional utilities, the costs of such preventive measures – whether in the form of "hardening" assets against attack, or ensuring that any disruptions to service are minimized by bolstering the resiliency of the system – would be accounted for in General Rate Case applications. Such costs would be separate from and additional to those incurred to meet Federal requirements for protecting critical infrastructure.

California electric IOUs appear to be well ahead of many of their peer organizations in North America and are serving as physical security innovators within the electric industry. Driven in part by NERC CIP-014 regulations, California IOUs are upgrading security operations centers and are "hardening" select transmission facilities (incorporating security upgrades that include perimeter fencing, electronic monitoring equipment, and improved access control). The IOUs are also continually testing new equipment to assess potential and cost-to-benefit tradeoff. Still, while California IOUs have demonstrated they are well ahead of many of their peer utilities, they have yet to attain their full physical security potential and competency. Similarly, the IOUs will need to continue to build their capacity in this area to assure they are well positioned to respond to an ever-shifting risk landscape.

This report concludes with recommendations for activities that would support a more robust program for assessing and bolstering both the physical security of key distribution assets and the resiliency of the distribution networks. Chief among these recommendations is that California's electric utilities – both investor-owned and publicly-owned – should assess their distribution assets and develop risk-based physical security plans. Specific staff recommendations on a Joint Utility Proposal raised in the R.15-06-009 rulemaking will be

reserved for the formal docket. This report, however, offers other ideas that may guide utility efforts to improving infrastructure security and cooperative policies.

## 1.1 Recommendations

- The informal Utility Physical Security Working Group formed for this proceeding (and which formulated the Joint Utility Proposal) should continue to convene and be encouraged to engage with the Commission and its staff.
- SED should forge stronger ties and rapport with key physical security partners with participation by the utilities and their working group.
- Actors responsible for California's electric grid physical security should share resources and data to improve monitoring of operations that span utility territories.
- California utilities, through the working group, should consider the value of, and report back to the Commission with an opinion on, available tools such as the Environment for Analysis of Geo-Located Energy Information (EAGLE-I) managed by the U.S. DOE, which inputs data directly from energy sector partners, performs big data analysis, and shares situational awareness data.
- California utilities should consider the value of, and report back to the Commission with an opinion on, U.S. DOE's new information classification system, "Critical Electric Infrastructure Information" (CEII) that facilitates voluntary sharing of critical electric infrastructure information between federal, state, and local government, and utilities.
- California electric utilities' regular planning and preparation for major outage incidents should incorporate physical security strategies.
- California electric utilities should be proactive to incorporate the latest modeling and quantitative risk analysis tools, methodologies, and expertise to record, categorize, and trend incidents to more thoroughly expose threats to the electric grid.
- California electric utilities should offer an opinion to the Commission on whether the U.S. DHS Security Regional Resiliency Assessment Program could have value in protecting California's distribution systems.

- To ensure more consistent physical security initiatives among the utilities, their security and response teams should identify those best practices which provide actionable steps for utilities to avert and respond to outage incidents.
- California electric corporations should form alliances to provide mutual aid and sharing of response resources when one or more members is in need of assistance due to an emergency incident.
- California electric utilities should be mindful of opportunities for grid architecture improvements when considering new security and resilience measures. There should be an emphasis on incorporating a menu of physical security strategies any substation from the time of its inception, including outright hardening of facilities, Protection in Depth (PID), and Crime Prevention Through Environmental Design (CPTED).
- When rebuilding, in response to an outage, utilities should embrace opportunities that often exist for improvements to the electric grid that go beyond mere in-kind replacement of prior infrastructure.

The Commission is considering a specific Joint Utility Proposal to establish individual Distribution Substation and Distribution Control Center Security Programs (Distribution Security Program). The joint proposal is focused largely on a process for utilities to assess their distribution systems -- primarily substations -- in terms of vulnerability to physical attack and ability to reduce adverse impacts. That proposal will be the subject of a separate SED Staff evaluation and proposal.

# 2 INTRODUCTION

The 2013 sniper attack on PG&E's Metcalf electric transmission substation south of San Jose[3] resulted in waves of concern felt from the halls of Sacramento to Washington, D.C. The incident sparked calls for tougher regulations to improve electric grid security standards, accountability, and transparency. The response at the Federal level came first, leading to additional provisions for Critical Infrastructure Protocols (CIP) that had been in effect for a decade. These were developed in a sweeping rulemaking by the Federal Energy Regulatory Commission (FERC).[4]

Specifically, FERC directed the North American Electric Reliability Corporation (NERC) to establish criteria for determining assets to be subject to CIP rules – which cover a gamut of security areas, including physical- and cyber security – resulting in new rules that bind electric utilities to employ physical security plans as a means to address vulnerabilities. The new NERC CIP requirements, CIP-014, apply to any asset deemed not redundant and for which, if failure occurred, cascading power failures could result. For electric substations regulated by FERC, this corresponds to applicable *transmission* substations.

California State lawmakers' 2014 response to the Metcalf incident took the form of SB 699 (2014 – Hill) [5] and centered on perceived gaps in CIP-014 that could potentially render *distribution* facilities vulnerable. In amending existing emergency reporting statutes, SB 699 directed the Commission to identify and address as appropriate any existent NERC CIP *potential vulnerability gap*, so as to provide assurance of adequate security safeguards for electric distribution systems.

[3] The April 16, 2013, late-night incident in which approximately 100 rounds of high-caliber rifle ammunition were fired at a PG&E transmission substation raised national awareness of the vulnerabilities of the electric infrastructure by physical attack. The perpetrators were not apprehended and remain at large. A sizable reward for information has been offered.

[4] The Energy Policy Act of 2005 (Energy Policy Act) gave FERC the authority to oversee the reliability of the bulk power system, including authority to approve mandatory cybersecurity reliability standards. NERC) which FERC certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

[5] Public Utilities Code Section 364 *(Amended by Stats. 2015, Ch. 612, Sec. 10. Effective January 1, 2016).*

The law further directed the Commission to consider adoption of new standards and rules to address any physical security risk to the distribution system of California's electric corporations so as to ensure continuous high-quality, safe, and reliable service. It also extended the Commission's enforcement authority over any utility non-compliance.

## 2.1 Commission Response to Legislature's Directive

The resulting Commission rulemaking (R.15-06-009) was initiated in June 2015, but accelerated in activity in early 2017, following a second pre-hearing conference and a scoping memo to frame the effort's objectives. SED staff conducted extensive research and outreach including conducting four public workshops around the state, interviews with experts in grid security, and tours of utility distribution facilities and control centers. These efforts better enabled staff to build a record, gain broader understanding of federal policy and California utility practices, and learn and hear from stakeholders and experts.

The proceeding has employed a research and workshop process to gather information and insights about the federal regulations and processes governing critical assets under the NERC/FERC program, and to hear from representatives of various agencies involved in electric physical security efforts – ranging from the Department of Homeland Security to the Federal Bureau of Investigation, and from the Western Electricity Coordinating Council to California's network of "fusion centers" that serve as information hubs for critical infrastructure.

The primary three issue areas addressed in this proceeding are 1) identifying a process for the prioritization of strategic electric facilities and determining appropriate security measures or approaches to ensuring resiliency of the system, 2) establishing practices for the exchange of highly-confidential or "sensitive" information between utilities and the Commission, and 3) confirming whether existing incident reporting requirements are adequate. These three subject areas are examined with an eye toward ensuring appropriate regulatory oversight of jurisdictional utility operational performance, and providing a mechanism for entities not subject to CPUC ratemaking authority to identify their own most appropriate measures.

Working in cooperation, utilities participating in the process – both investor owned utilities and publicly owned utilities and co-operatives – have reached consensus on a Joint Utility Proposal to establish individual Distribution Substation and Distribution Control Center Security Programs (Distribution Security Program). The joint proposal is largely focused on a process for utilities to assess their distribution systems, primarily substations, in terms of vulnerability to physical attacks and ability to reduce adverse impacts. That proposal has been circulated to the Service List of this rulemaking, and will be the subject of a separate SED Staff evaluation and proposal.

This White Paper report will not specifically address the Joint Utility Proposal, as it is subject to Commission consideration and possible refinement in the rulemaking. This report is more concerned with the status of industry efforts to ensure physical security to date, and provides background that that has framed the utility proposal, and that will inform the Commission's future policy determinations. Any recommendations for continued actions by utilities and the Commission presented here do not need to be adopted by the Commission or codified within Commission policy at this time.

## 2.2 Summary of Staff Assessment of Risks Surrounding Distribution Assets

Because of the experience gained as electric utilities have implemented the federal program for critical infrastructure protections, California's electric system operators have already identified their most critical assets for vulnerability, and have taken steps to increase security via "hardening" of (primarily transmission) substation facilities, as well as improvements to security measures, such as video surveillance, alarms and patrols. Already, California's jurisdictional utilities have sought approval for millions of dollars in General Rate Case funding to ensure physical security and compliance with CIPs.[6]

The next level, determining proper policies and procedures for distribution-level assets, needs to be understood in the proper context. Even a coordinated attack against distribution facilities

[6] A separate and much larger amount of funding for utility physical security efforts is linked to Federal compliance efforts authorized by FERC rates.

is unlikely to result in widespread system disturbances or cascading outages, owing to the local grid's built-in redundancy and the relatively small service share typically assigned to any single distribution substation.[7] Depending on the design of the distribution system, redundancy can be built into system so that a distribution circuit can be served by an alternative substation if the primary substation experiences an outage.

Sound security practices for utility distribution assets are not predicated on how well defended these assets may be. Rather, there should be a balance between infrastructure and security improvements – preventive measures – and ensuring the resiliency of the distribution network.

Thus, effective risk mitigation could be made to address both the likelihood of an adverse event, such as a Metcalf-like attack, *and* reduce the potential consequences of an incident. This approach is valuable, not just for addressing physical security, but also for reducing impacts from weather events as well as the notorious catch-all "other" category-of-causes of system disturbances.[8]

The nature of these facilities individually, as comparatively expendable, and the high cost that would accompany any comprehensive attempt to fortify them to a level that would render them impermeable, makes the prospect of categorically "hardening" these assets impractical and cost prohibitive.[9]

California's existing IOU distribution substations generally exhibit multiple characteristics that render them low-value targets that would be prohibitive to categorically defend or harden.

[7] Substation density ranges from one per 100 square miles in PG&E service territory to one per 270 square miles in SCE service territory. A PG&E distribution substation serves an average of 7,600 customers per substation; a SCE distribution substation serves an average of 82,000 customers per substation. Distribution substations range from a small rural substation with a nominal rating of 5 megavolt ampere (MVA), to an urban station may be over 200 MVA.

[8] For example, in 2015, a squirrel came into contact with substation equipment and caused a two-hour-long outage incident that impacted 45,000 customers from Richmond to Berkeley.

[9] Additionally, staff opinion holds that even if a distribution substation were to be fortified as a walled fortress facility, their assets would still be vulnerable to a determined attacker. Additional significant costs on-site security guards would likely be necessary to deter intrusions or attacks. Even armed guards would not be able to defend against a military-grade coordinated attack.

These include:

- Voluminous (a number exceeding 300, counting IOUs alone);
- Moderately to highly redundant;
- Relatively dense in their siting and typically spaced within of a few miles of one another;
- Located within urban areas of moderate to high density;
- Compact in footprint area, typically consuming no more than one-quarter to one acre;
- Able to be repaired fairly quickly (typically within a week or less); and
- Difficult to defend against a well-prepared and determined attacker.

These characteristics argue against attempting to employ a "one size fits all" strategy for physical security. Instead, the best approach would appear to be one that affords some flexibility while stressing the value and importance of: 1) assessing facilities for their contribution to system reliability and nature of load served, 2) evaluating their vulnerabilities to intrusion, attack or other disturbances, and 3) ensuring redundancy in the local system in the event of an adverse incident.

In this report SED staff offers a list of recommended strategies and proposed new utility practices as practical and low-cost reforms that help make the grid more secure without unduly raising consumers' electric bills.

# 3 Electric Utility Physical Security in the Post-Metcalf Era

## 3.1 Role of Distribution Substations and Typical Facility Description

In many regards, distribution substations are the motherboards of the electric grid, effectively providing the path of flow for energy along pre-determined networks circuitry. Distribution substations have the important role of converting and lowering primary voltages from the transmission system -- which in California can range from primary voltages from 69 kilovolt (kV) to 500 kV -- to secondary voltages on the distribution system, ranging from 2.4 to 34.5kV.

California's combined count of electric transmission and distribution substations exceeds 3,200 across its several dozen electric utilities, whether investor- or publicly-owned entities. SED staff estimates the total distribution substation number at about 2,000.[10]

The California distribution systems were built in the period from the late 1940s to the 1970s, when the population grew from 7 million in 1940, to 22 million in 1975. The electric grid followed the population's migration to the suburbs and beyond, with distribution substations serving as the critical link from primary to secondary service; from the transmission line to the customer meter.

During this period -- 1946 to 1953 – Pacific Gas and Electric invested over $1 billion in new system facilities, representing the most rapid large-scale utility expansion ever for a U.S. energy utility.[11, 12] During this period, California electric utilities built thousands of miles of electric line extensions and associated distribution substations.

These legacy substations and their hardware have not changed much since construction, and the era in which they were built was little, if at all, concerned with potential terrorist attacks. Facilities were (and in many cases, still are) often fully visible to the public, often located close to voltage load centers, and without much of a protective barrier apart from chain link fencing and perhaps barbed wire.

## 3.2 Typical Distribution Substation Description

A typical distribution substation is relatively compact, with an area of less than one acre in urban areas to a few acres in rural locations, and is enclosed by 6-to 8-foot-high chain-link fencing. In dense urban areas such as San Francisco or downtown L.A., a substation may be enclosed within a building shell. In residential or commercial areas, substations they are usually screened to make them less conspicuous. Tall landscaping acts as a visual barrier, obscuring

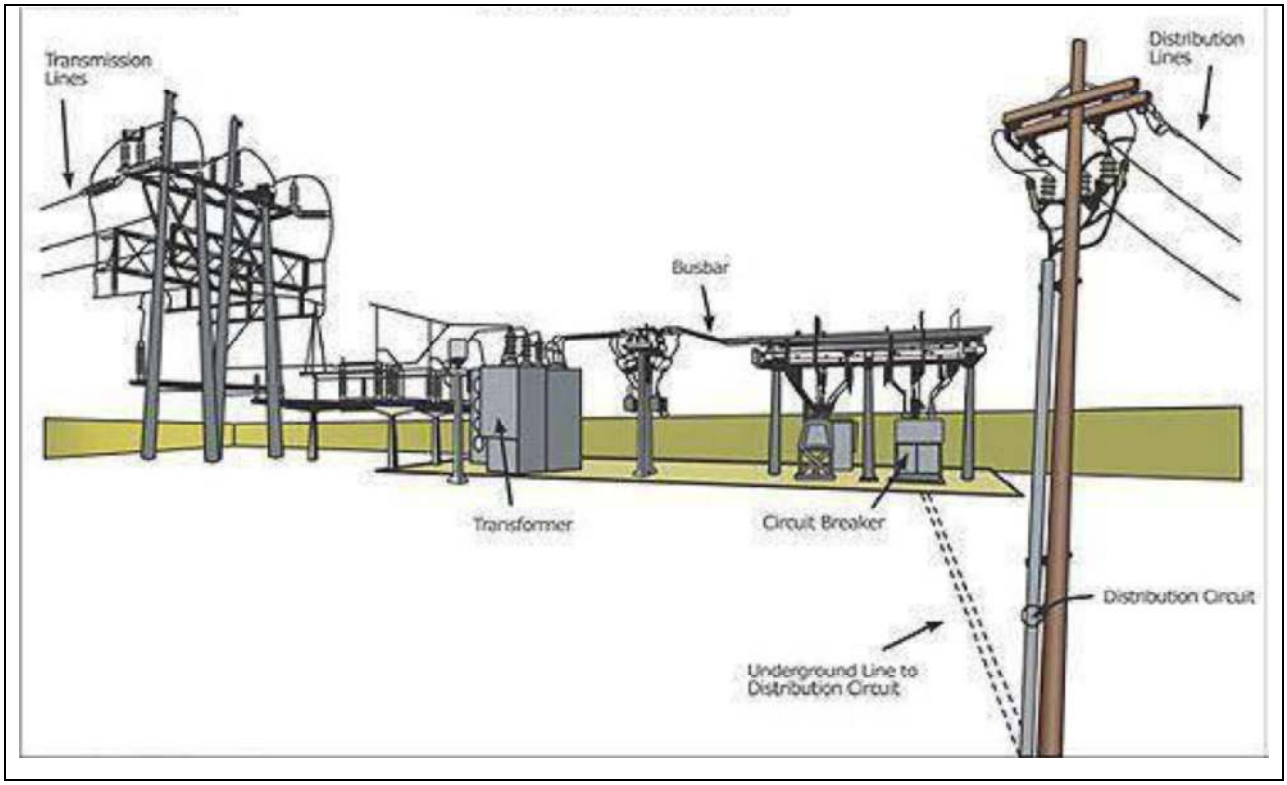
[10] Data request responses by the three major investor-owned utilities put the count of distribution substations at 1,500. The 2,000 count would include those owned by POUs (municipal electric utilities).
[11] 1950s dollars, equivalent to over $10 billion in 2017 dollars assuming annual inflation rate of 3. 53 percent.
[12] Coleman, Charles, *PG and E of California, The Centennial Story of Pacific Gas and Electric Company 1852-1952*, McGraw-Hill, 1952.

assets from public view, but offering screening to intruders. In the case of adjacent mature trees, high branches and limbs may serve as a ladder into the facility.

In urban areas, it is not uncommon that a substation is sited adjacent to a neighboring residential or commercial use. For urban substations, razor wire is frequently applied atop fencing as an extra security measure. A facility in a rural setting would typically be isolated, creating a different set of issues surrounding security and incident response.

The volume of distribution equipment and complexity of hardware at substation facilities vary, but they are generally sized and built to meet the existing and anticipated electric service needs of the nearby community. Although size and load capacity will vary from facility to facility, substations largely share consistency of design and configuration. Most substations feature similar equipment, switchgear, circuit breakers, transformers, and communication and control systems designed to operate safely and seamlessly in providing electric service.

**Figure 1. Distribution substation component hardware**



Inside the substation, one will often find a control building containing control panels and other equipment used to operate the substation. These structures are often fortified to thwart entry. At least two transmission lines feed the substation, most often from overhead lines.

The other item that immediately catches one's eye are the transformers – the workhorses of the distribution system – which typically stand over eight feet in height. Substations in more densely-developed areas will have multiple transformers to enable greater operational capacity, flexibility, and resilience. In rural areas a substation may have just a single large three-phase oil-cooled transformer mounted on a concrete pad that rises from a dirt floor. Transformers at distribution facilities (and at transmission substations) are encased in heavy-gauge steel, rendering them resistant to tampering or attack. It is their external radiators that present a vulnerability.

### 3.2.1 Common Security and Threat Issues Surrounding Distribution Substations

Common-sense, low-cost solutions appear to hold great potential for increasing the security of these facilities. Particularly in remote areas, substations are often secured with a chain and padlock, as they have been since being constructed decades ago. During one SED staff visit to a distribution substation in the Central Valley, utility staff told of a security incident triggered when a contractor working late one night at a substation neglected to close and lock the gate. Later that night an intruder entered the substation. Fortunately, utility staff were still working on site, and were able to promptly notify law enforcement.

At another utility, a former employee did not surrender his utility keys upon termination, which enabled a physical security incident. The disgruntled former employee entered a substation one night and set fire to a transformer and control building, causing damage that exceeded $1 million. As a result, the utility since has adopted "smart lock and key" procedures.

At a Southern California substation visited by SED staff, sections of chain-link fencing cut to force entry to the property were evident. The utility had placed temporary patches over these sections of fence. Along this side of the facility, the substation shared a property line with a

heavily-vegetated parcel that had a flood-control swale and dirt path, which facilitated vandals' access to the utility property without being detected.

Although substations in urban areas are often targets of vandalism and trespassing, given the typical low impact of these threats to distribution reliability, existing security measures may be minimal. This contrasts greatly with what may be found at a larger scale facility that has been determined to be critical for system reliability.

## 3.3 Hardened Facility Example

### 3.3.1 Electric Transmission Substation, Hypothetical Example

*The following "hardened" facility description of an electric transmission substation site, drawn from multiple SED staff site visits to utility substations in 2017, is a composite and is provided here for illustrative purposes as an example of what might be considered the state of the art in measures for protection for such facilities. The example here is provided without regard for cost, which may be extensive or prohibitive.*

After driving to the edge of a non-descript, low-density exurb, the vehicle turns off the main arterial and on to an unsigned two-lane road that quickly drops behind rolling hills. After perhaps a quarter mile, passage is blocked by a heavy-duty swivel-arm vehicle gate extending across the road. The gate, of the type frequently employed by the U.S. Forest Service on restricted access roads, is secured by padlock and intended to limit access by cars and trucks. It is here that a utility property notice is posted. The road appears open to pedestrians and bicyclists.

The area immediately surrounding is arid, dusty, and what limited vegetation exists appears as primarily scrub brush and chaparral. No tall or dense groves of trees obscure visibility to the facility. Just outside, there is a parking area, past a chain-link swing-open gate.

Outside the facility, overhead transmission lines are strung along a parade of steel towers converge from several different directions, with larger towers bringing in electrical energy from the regional grid to the substation.

The facility is protected by a large 10-foot-high prefabricated reinforced panel or cinderblock wall. The wall has a single point of ingress/egress, which is defined by a solid reinforced (approx. 4,000 lb.) rolling door that when opened, retracts into the facility so as to be flush with the wall. The door, so heavy it requires a dedicated 220-watt power line to power its large motor, is capable of withstanding most any ramming attempt by a typical speeding passenger vehicle.

The transmission substation site is perhaps 20 acres in area with the outside grounds covered by a porous, small-rock material. The site is composed of distinct areas; the site covers a lot of area and its limited contents are spaced far apart. At one side far from the gate are simple and compact windowless one-story structures containing office work areas, office equipment, and manual control equipment. Other similar clusters of structures for training, research and demonstration testing, and other utility business lines may be present within various areas on the margins of the site.

At yet another edge of the facility is a large, 40-foot-high, perhaps 50,000-square-foot warehouse building that resembles an airplane hangar. It contains sensitive hardware – inert gas-cooled transformers that require more constant temperature control and protection from the elements.[13] Such hardware, if unenclosed, would be highly-vulnerable and attractive to would-be attackers.

Between the hangar-like structure and the high, defensive perimeter wall is a tall rack of electronic devices consisting of seven columns of protective switches (used for isolating the transformers from the outside circuit to allow for offline maintenance). This general grade of rack is found elsewhere within the site perhaps three or four times.

In the center of the site are the facility's most vulnerable and costly assets – the transmission transformers – located in the open air. They number perhaps ten in number, have conspicuous multiple fans to aid their oil-cooled external radiators, and each consumes an area on par with a good-sized house.

[13] This gas is relatively rare and requires a special license to obtain and operate. This SF6 gas, if released into the atmosphere would degrade the ozone layer, similar to consumer-level CFCs.

Linking the various assets are connected trenches and vaults covered with metal grating. Their perimeter ropes appear to form designated walking paths. In fact, the ropes are intended to keep personnel off the grating areas, which are reserved for making repairs and for catchment of spilled or leaked cooling oil.

Not uncommon for transmission substation sites at the edge of urban areas, this facility has adjacent to it a vast utility stockyard of perhaps four acres. The stockyard, consisting of sheds storing tools and spare parts, contains bulky hardware and materials stored in the open air. The stockyard shares one wall with the substation; its remaining edges are defined by 10-foot-high chain-link fencing.

Outside the wall, a defensive inner-ring buffer zone twenty to fifty yards deep is defined by a 10-foot-high chain-link fence, topped with razor or barbed wire, encircling the immediate outside grounds. It is within this inner-ring buffer that, ideally, any telecommunication vaults or other critical telecommunication infrastructure servicing the facility and not within the inner wall would be sited. Terrain both within and outside the inner-ring buffer zone is cleared of vegetation and other features that could serve to conceal a threat. Additional primary protective raised barriers in the immediate site area may include man-made earthen berms. Remaining utility-owned acreage surrounding the facility but outside the inner-ring area, serves to create yet an additional buffer area between public space and private property. The immediate surrounding area is well lighted with illumination directed outside the walls and away from assets and onto the inner-ring and outer buffer areas.

From outside the facility, the site appears as a well-guarded and impermeable fortress. Conspicuous warning signs are posted at the gate to the chain-link fence and at regular intervals along the fence. The heavy gate would be reinforced with a heavy padlock or preferably with controlled electronic gate access that monitors and records all entries into the facility.

From the gate and fence, security measures and implements are observable in the vicinity of the wall. These include various cameras (most of which are able to pan, either automatically or

by remote operation), gunshot and motion detectors, a PA system, and barbed wire and/or dagger-like spikes affixed to the top of the wall.

Unseen would be subterranean vibration or seismic detection sensors in the ground below and outside the wall. Additional internal and external detection capacities might include video recognition and analytics, and an ability to detect and track approaching unmanned aerial vehicles (UAVs or drones).

Depending on surrounding outer topography characteristics and sight vantage into the facility, the substation might also incorporate limited placement of 25-foot-high armor shielding to protect the most vulnerable transformer assets from rifle fire by all but the most high-caliber ammunition.

Electronic keys and locks hardware and protocols outside and within the wall of these hardened facilities are one of their most fundamental security features and incorporate smart keys[14] whose access is restricted and can be rapidly reassigned as situations and authorized personnel shift.

Note that these hardened facilities are typically not occupied after normal business hours. As facilities largely controlled by remote central command operators, they may or may not have a large utility staff presence during work hours depending on regular and intermittent ancillary activities they may host such as training and drills, maintenance, storage, and demonstration technologies.

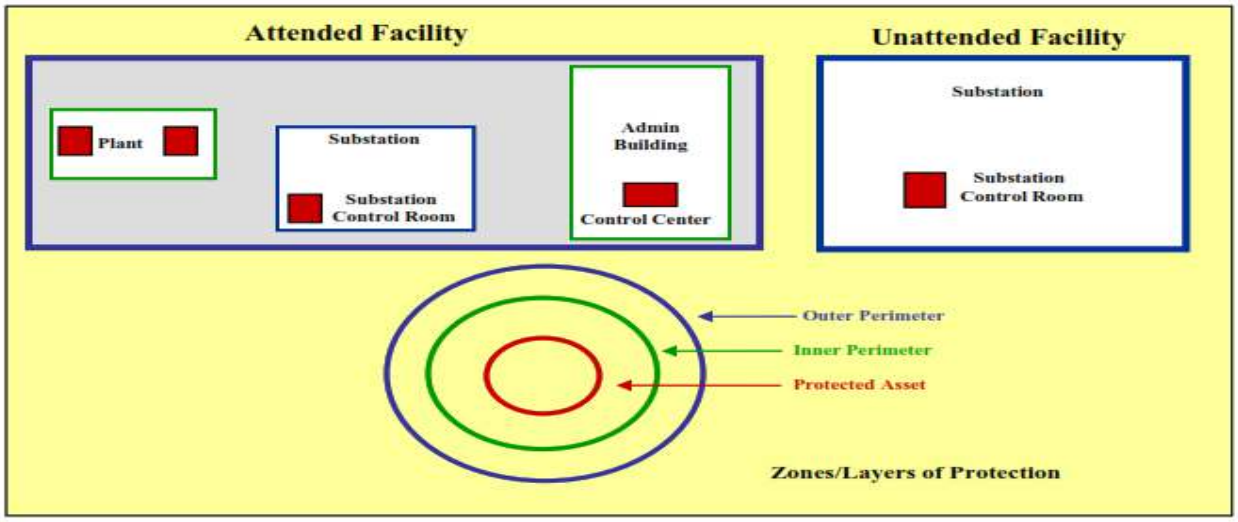
It is clear that this is a thoroughly modernized facility, designated one of California's critical infrastructure assets for its indispensable role as a central hub of the high-voltage network, and afforded a level of protective security measures commensurate with its importance to system reliability.

[14] Generally, such keys can be reassigned and reprogrammed remotely.

## 3.4 Alternatives to Facilities Hardening

Relatively low-cost physical security strategies that rely less on outright hardening and instead attempt to buy response time by slowing an attack's progress, or that aim to deter crime by projecting a sense of a highly-ordered environment, have been gaining traction in recent decades. One, Protection in Depth, or PID, looks to deter, delay, and ultimately frustrate any would-be attacker by situating a facility's most important assets in the center of a series of concentric defensive zones that each must be breached. Such a sequence of barriers, increases the likelihood of, if not outright confounding an attack, at least would allow time for a response.

**Figure 2. Diagram of a Protection-in-Depth Placement of Assets**




**Source:** NERC, Electric Physical Security Guideline

NERC sums up PID as "a strategy that seeks to delay rather than prevent the advance of an attacker, buying time by yielding space. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on the tendency of an attack to lose momentum over a period of time . . ." [15]

[15] Security Guideline for the Electricity Sector: Physical Security, NERC, v. 1.9, last revised 2011. Available for download at: http://www.nerc.com/comm/CIPC/Security%20Guidelines%20DL/Physical%20Security%20Guideline%202012-05-18-Final.pdf

A second alternative-to-outright-hardening, "Crime Prevention Through Environmental Design" (CPTED), by contrast, leverages physical orientation and encourages visibility to reduce opportunities for crime and to signal that disorder is not tolerated.

CPTED draws from sociology, architecture, and law enforcement to assess how site conditions and the natural and built environments surrounding a site area may contribute to or deter opportunities for crime. CPTED typically seeks to 1) limit access to a facility by means of a single portal, 2) advance opportunities to see and be seen, and 3) project a strong sense of "territoriality," ownership, upkeep, and sense of order.

There are researchers[16] who caution that a hazard exists for a corrupting "dark side" of CPTED to emerge when structures are "over-hardened" such that they come to resemble fortresses. Such buildings particularly in urban environments, can have unintended consequences by signaling that the outside world is chaotic to the point of necessitating it be shut out.[17]

## 3.5 Key Partner Agencies in Electric Physical Security

The nine entities detailed in **Table 1**, below, play key roles in ensuring the security of the nation's electric grid. These entities' contributions include rulemaking, regulatory enforcement, law enforcement and intelligence gathering, and emergency response.

**U.S. Department of Energy (DOE)**

The U.S. Department of Energy provides support and resources to improve physical- and cyber security and resilience. U.S. DOE's role includes supporting the Electric Sector Coordinating Council, a public-private partnership that supports threat information sharing, and R&D.

[16] Cozens and Love, Oxford University Press, 2017

[17] These fortress-like structures typically have exterior walls with the first 15 feet of elevation displaying few if any openings. In San Francisco, one striking example would be PG&E's Embarcadero substation, a fortress-like edifice with a forbidding street presence.

U.S. DOE is considered to be the nation's most complete source for information on physical security incidents, thanks to its OE-417 Electric Emergency Incident and Disturbance reporting program.

**Federal Energy Regulatory Commission (FERC)**
FERC is the Federal agency that oversees the interstate transmission of energy in the U.S., including natural gas, oil, and electricity as afforded by the Federal Power Act. Responsibilities include approving reliability standards for bulk power systems to address physical- and cyber security. FERC also certifies Electric Reliability Organizations (EROs, such as WECC, detailed below), which are responsible for the monitoring and enforcement of these standards at the regional interstate level.

**North American Electric Reliability Corporation (NERC)**
NERC is an NGO that reports to FERC and is responsible for carrying out federal rules surrounding reliability and security of the bulk power transmission system in North America. It oversees eight regional Electric Reliability Organizations that monitor and enforce compliance with NERC/FERC rules. NERC also provides reliability standards for power systems, including the protection of critical infrastructure. NERC has 14 critical infrastructure protection (CIP) standards, 13 of which address cyber security and one standard, CIP-014, to address physical security. NERC operates the Electricity Information Sharing and Analysis Center (E-ISAC) which offers security data services to bulk power system owners and operators.

**Western Electricity Coordinating Council (WECC)**
The Western Electricity Coordinating Council is an NGO regulatory authority responsible for coordinating and promoting system reliability for the Western Interconnection, a territory that includes 14 U.S. states, two Canadian provinces, and a northern portion of one Mexican state. WECC is the regional compliance enforcement agent for NERC, and to ensure compliance with CIP-014, it conducts audits of utilities' CIP security plans and implementation practices.

WECC supports a *Physical Security Working Group* that meets every six months and consists of about 60 members representing utilities in the Western U.S. The working group exchanges information on physical security best practices including security metrics, active shooter protocols and training, new security technologies, and advanced design. Of particular note, this

group has provided support to member utilities on CIP 014 compliance, and conveyed Federal updates. The working group also serves liaison between utilities and WECC and the NERC *Critical Infrastructure Protection Committee*.

**Governor's Office of Emergency Services (Cal-OES)**
The Governor's Office of Emergency Services (Cal-OES) oversees and coordinates emergency preparedness, response, recovery, and homeland-security activities for the State, including the State Threat Assessment Center (STAC), an information clearinghouse directed to strategic threats. Cal-OES administers and disburses over $1 billion annually in grant monies made available from the U.S. DHS.

**U.S. Department of Homeland Security (DHS)**
The U.S. Department of Homeland Security provides alerts on active threats, supports state and local efforts to develop strategies, and provides resources to mitigate physical security incidents, including Regional Threat Assessments, security and technical expertise, and grant making. DHS maintains a *National Infrastructure Advisory Council* and a *Critical Infrastructure Partnership Advisory Council* that coordinate infrastructure-protection public-private partnerships.

**Federal Bureau of Investigation (FBI)**
The Federal Bureau of Investigation investigates suspected terrorist threats and major criminal activities. Physical security incidents that impact the grid are assigned to the FBI's Joint Terrorism Task Force.

**Local Law Enforcement**
Local law enforcement is typically dispatched to any distribution facility where an event has been reported in order to assess the threat to public safety and determine an appropriate police response. In most cases, local law enforcement must be in communication with the distribution owner to adequately respond to a physical security threat.

**Fusion Centers**
Fusion centers operate as the State- and major urban center-level for the gathering, analysis, and sharing of threat-related intelligence among Federal, State, local, and industry partners. Fusion centers ensure real-time dispatch of threat information and analysis essential to

ensuring effective homeland security. They provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They also provide training, technical support, and grant funding. In California, the State Threat Assessment Center (STAC) in Sacramento is the lead for fusion center for State-level threat tracking and serves as California's information sharing clearinghouse of strategic threat analysis and situational awareness reporting. In addition, five regional fusion centers interface with STAC to comprise the State Threat Assessment System. [18]

[18] The regional centers are located in Sacramento (Central California Intelligence Center), San Francisco (Northern California Regional Intelligence Center), Los Angeles (Los Angeles Joint Regional Intelligence Center), Orange County (Orange County Intelligence Assessment Center), and San Diego (San Diego Law Enforcement Coordination Center).

**Table 1. Key Physical Security Partner Agencies**

| Entity Name | Entity Abbreviation or Shorthand | Entity Mission and Purpose | Entity Function within Electric Physical Security | Entity Contribution to Phase I of Proceeding | Public, Private, or NGO | Federal, State, Regional, or Local |
|---|---|---|---|---|---|---|
| U.S. Department of Energy | **U.S. DOE** | Oversees U.S. coal and nuclear energy and weapons sectors | Oversees all activities associated with the National Infrastructure Protection Plan and Energy Sector Specific Plan | no involvement | **Public** | Federal |
| .S. Department of Homeland Security | **U.S. DHS** | Multiple federal agencies with roles in protection of homeland security including counterterrorism, cybersecurity, protection of critical infrastructure, and response to major events | Supports State and Regional entities with regional risk assessments and threat & vulnerability assessments | Fusion Center rep spoke at Workshop 1 | **Public** | Federal |
| Federal Bureau of Investigation | **FBI** | Law Enforcement | Investigation of physical security incidents that impact interstate commerce or have significant impact on public safety | Staff spoke about agency programs in closed session informing Workshop 1 | **Public** | Federal |

| | | | | | | |
|---|---|---|---|---|---|---|
| Governor's Office of Emergency Services | **Cal-OES** | Supports and informs all phases of emergency management including preparedness, response, recovery and mitigation. | Would be brought on in the event of a prolonged significant event to aid recovery and emergency response | Leadership spoke at Workshop 1; provided facility for Workshop 1 | **Public** | State |
| Local Law Enforcement | **County Sheriff or City Police Department** | Law Enforcement | Coordinates with and supports utilities in case of physical security event. Provides training for utility physical security and emergency response | no direct involvement, some utility security personnel are former local law enforcement | **Public** | Local |
| Intelligence Assessment Centers and Joint Regional Intelligence Centers | **Fusion Centers** | Law Enforcement | Focal point for the receipt, analysis and sharing of threat-related information among all levels of law enforcement. Six fusion centers located within California | Briefing to SED on Cal COP information platform at the Northern California Regional Intelligence Center | **Public** | Federal |

| | | | | | | |
|---|---|---|---|---|---|---|
| North American Electric Reliability Corporation | **NERC** | not-for-profit organization that develops and enforces Reliability Standards for electric industry | Develops reliability standards regarding critical infrastructure protection for bulk power system in US. Also hosts biennial exercise, GridEx, simulating cyber/physical attack on electric infrastructure. | Presented at Workshop 2 on CIP 014 | **NGO/quasi-governmental** | Interstate, international in scope |
| Federal Energy Regulatory Commission | **FERC** | regulates bulk power system, interstate transport of electric power, natural gas, and oil | Statutory authority over physical security of bulk power system with adoption of Physical Security Standard, CIP-014 | no direct involvement | **Public** | Federal |
| Western Electricity Coordinating Council | **WECC** | Serves as regional arm for NERC/FERC compliance, enforcement, and promotion of transmission system security within the Western Interconnection | As Electric Reliability Organization, WECC monitors and enforces reliability standards through physical security audits | Presented at Workshop 2 on audit procedures | **NGO/quasi-governmental** | Regional; interstate, international in scope |

## 3.6 Electric Physical Security Context Prior to 2014

Before the California and Federal responses to the Metcalf incident, electric utility physical security in the United States was voluntary, and largely limited to monitoring physical security incidents. For example, in 2001, the North American Reliability Corporation (NERC) issued its document "An Approach to Action for the Electricity Sector," which provided guidelines to physical security for electric utilities. [19] The document describes a tiered approach that promoted concepts such as "Defense in Depth" and "Crime Prevention Through Environmental Design," which are discussed later in this chapter. Similarly, the Institute for Electric and Electronic Engineers (IEEE) in 2000 published its own guidelines, "1402-2000 - IEEE Guide for Electric Power Substation Physical and Electronic Security."[20]

Federal-level attention to cyber security intensified after a series of high-profile banking fraud incidents involving organized offshore crime rings that had netted tens of millions of dollars from U.S. financial institutions. Year 2003 was notable for the homeland security-driven "Presidential Directive HSPD-7 for Critical Infrastructure Identification, Prioritization, and Protection," as well as NERC's debut of its inaugural cyber security guidelines. Commonly referred to as the NERC Critical Infrastructure Protection (CIP) plan, these information security standards for the electrical power industry came to be known as NERC CSS (Cyber Security Standards).[21]

At around the same time, concerns about the physical security of electrical assets were elevated by a sharp rise in metal theft incidents. The crime increase was attributed to a spike in copper prices that rendered copper wiring more valuable and attractive to would-be thieves. However, copper prices settled back to more traditional cost levels, and since the agency's last report in the late 2000, the U.S. DOE has been silent on the issue.

In 2010, the National Infrastructure Advisory Council, in conjunction with the U.S. Department of Homeland Security (DHS), issued "A Framework for Establishing Critical Infrastructure

[19] Available for download at http://www.iwar.org.uk/cip/resources/nerc/cip-nerc.pdf
[20] Available for download at http://ieeexplore.ieee.org/document/836296/
[21] Some iterations later, the version in effect in 2017, is called CIP-002-3 through CIP-009-3, and applies to the bulk power system.

Resilience Goals."[22] The paper defined *resilience* as the ability to reduce the magnitude and/or duration of disruptive events. The report noted the potential for public agencies to enhance the resilience of the electricity sector, including aligning Federal and State governments in policy, planning, standards and regulations; and improving access to information regarding threats

In February 2013, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21) and Executive Order (EO) 13636, established Federal agencies' roles regarding physical- and cyber security threats. These policies reemphasized the need for a novel collaborative approach to security and risk assessment, with the U.S. DOE overseeing issues related to the electric utility sector via the newly-formed Electric Subsector Coordinating Council (ESCC).[23, 24]

## 3.7 Federal Action and NERC CIP-014

As described above in the Introduction chapter, new NERC physical security standards were adopted in 2014, under CIP-014 for the bulk power system. These rules established a risk-based protocol that identifies critical transmission assets and control centers. In contrast to previous NERC-issued guidelines, CIP-014 authorized FERC to establish one mandatory physical security standard for the nation's transmission assets.[25]

To recap, the first security "standard" was developed and issued by the IEEE in 2000. In 2002, NERC issued guidance that provided information on voluntary physical security measures. The

[22] Available for download at https://www.dhs.gov/xlibrary/assets/niac/niac-a-framework-for-establishing-critical-infrastructure-resilience-goals-2010-10-19.pdf
[23] More at http://www.electricitysubsector.org/
[24] A Federal-level example of government-utility partnerships, Electricity Subsector Coordinating Council (ESCC) serves as liaison between the federal government and the electric power sector. As a result of the cyber attack on Ukraine's grid assets in December 2015, the ESCC asked the North American Transmission Forum (NATF), a trade association representing transmission owners, to assess the operating strategies and reliability tools available to the electric power industry should the operations of the bulk electric system be compromised. NATF's assessment included operating strategies and reliability tools available to operators during such events. Similarly, ESCC, in collaboration with the American Gas Association, developed a "Ransomware Preparedness" document for energy companies that may reduce the risk and associated impacts of ransomware. A separate tool recently co-developed by industry and NERC is the Electricity Information Sharing and Analysis Center (E-ISAC), a secure means of sharing information, improving situational awareness, and communication among all parties during an event.
[25] CIP-014 applies to transmission facilities above 500 kV, or those facilities between 200 kV and 499 kV having "aggregated weighted value" greater than 3,000 kV.

Energy Policy Act of 2005, represented the first time the development of utility security standards were mandated, specifying expectation for cyber security protocols. The Federal government then produced a "National Infrastructure Protection Plan**,"** issued by the DHS in 2006. The plan described how public-private partnerships were to advance the resilience of critical infrastructure community to address security risks. Subsequently, in 2007, FERC issued new regulations under Section 215(d)(1) of the Federal Power Act (FPA), establishing eight Critical Infrastructure Protection (CIP) Reliability Standards.

The CIP Reliability Standards outline criteria that Bulk Power Transmission System utilities must follow to safeguard critical cyber assets. In March 2014, FERC directed NERC to develop a physical security reliability standard for the bulk power system. In November 2014, FERC advanced new regulations within established CIP Reliability Standards for physical security, Reliability Standard CIP-014-1, enforceable by law and subject to penalties for non-compliance. Because CIP-014-1 was issued with an 18-month period allowing for utilities to become compliant, and with somewhat arcane provisions describing a FERC directive to NERC to clarify certain language, CIP-014-2 became effective as the nation's first physical security standard to govern electric utilities.

The CIP-014-2 standard was made effective by FERC in May 2015, and clarified that only assets with a "critical impact" would be required to conform to the standard, which relies on a complex set of security plan requirements that entail assessing assets and potential threats, outside expertise and peer review, proposed mitigation measures and validation, and site inspections and security plan audit cycles. A complete review of CIP-014 requirements is beyond the scope of this report, but further details about guidelines and requirements are provided in **Appendix 1**.

In the time since CIP-014 became effective, electric utilities have responded by initiating the process with FERC's designated regional compliance authority or ERO to first determine whether any asset holdings would be subject to CIP requirements. If found to be subject to the rules – wholly based on whether assets are deemed critical – utilities would be advised to initiate the lengthy physical security plan audit process.

### 3.7.1 DHS Technical Services in Support of Security Plans and CIP-014

To support bulk-power system owners and operators in their compliance with NERC/FERC CIP-014 standards, DHS offers a *Physical Security Program* (PSP) to facilitate development of security plans for critical infrastructure. The program is voluntary and separate from Federal regulatory activities.

DHS commonly assists electric utilities on a voluntary basis with identification of gaps in infrastructure security. DHS Protective Security Advisors are available to conduct site visits at individual assets to probe existing physical infrastructure, identify vulnerabilities, and locate solutions.

DHS staff reviews of existing procedures and physical security plans -- to offer an independent third-party opinion -- is a second DHS compliance-services offering. Upon completion of such a facility gap analysis, a revised physical security plan can be finalized by the transmission owner or operator for audit and validation by WECC or another ERO.

**Table 2** below details DHS offerings to support critical infrastructure security and resiliency, including the agency's Infrastructure Survey Tool, a web-based security survey directed to owners and operators to enable critical infrastructure assessments. With more than 100 questions to gauge security management, information sharing, and protective measures, the survey aids in the identification of vulnerabilities and appropriate mitigation measures.

DHS reports that they are finalizing a means of sharing such vulnerability assessment data with a broader spectrum of stakeholders, which might include Commission staff.[26]

[26] U.S. General Accounting Office, *DHS Risk Assessments Inform Owner and Operator Protection Efforts and Departmental Strategic Planning,* GAO-18-62, October 2017.

**Table 2. Select DHS Risk Information Products and Services**

| Vulnerability Assessment Actors and Products/Activities | Explanation and Information Sharing Mechanism (if applicable) |
|---|---|
| **National Protection and Programs Directorate - Protective Security Advisors (PSAs)** | |
| Enhanced Critical Infrastructure Protection (ECIP) Visits | PSAs conduct these visits with critical infrastructure (CI) owners and operators to establish DHS's relationship with the facility and communicate available infrastructure protection services that could enhance their security. |
| Infrastructure Survey Tool (IST) | The IST is a web-based security survey intended to assess a facility's vulnerabilities. Conducted by a PSA in coordination with facility owners and operators, it identifies facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery. |
| Rapid Survey Tool | This vulnerability assessment survey is a web-based data collection capability that examines the most critical aspects of a facility's security and resilience posture with baseline questions. The results are analyzed to determine the facility's relative security and resilience in comparison to the national average for similar facilities. |
| Infrastructure Visualization Platform (IVP) | IVP is a data collection and presentation medium that supports critical infrastructure security, special event planning, and responsive operations. It provides immersive imagery, geospatial, and hypermedia data of critical facilities, surrounding areas, transportation routes, and more. It also integrates assessment data from other PSA assessments. |
| Regional Resiliency Assessments Program (RRAP) | RRAP is an assessment of critical infrastructure within a designated geographic area and a regional analysis of the surrounding infrastructure to address a range of infrastructure resilience issues that could have regionally and nationally significant consequences. |

**Source:** U.S. General Accounting Office

### 3.7.2 NERC Technical Services in Support of Security Plans and CIP-014

NERC provides direct support to electric utilities to increase their understanding of the various requirements in CIP-014, and promote transparency and integrity as the industry moves to implement the standard. NERC offers coaching and tutoring on CIP requirements and security plan rigor, on a voluntary and informal basis with utilities to promote robust compliance and partnering. Included in the menu of services are physical security site visits by NERC physical security advisors. NERC officials' presentation at the May 31, 2017, CPUC physical security proceeding workshop described having provided assistance to 19 entities in six U.S. electric grid regions of the US as of August 2016.

Common themes addressed in these collaborations include:

- Timelines for implementing security and resiliency measures
- The role of third-party reviewers and at what stage in the CIP-014 process
- Scope of security plans
- Insider threat concerns
- Confidentiality of information

In addition, NERC conducts a biennial security exercise, GridEx. First initiated in 2011, the 2017 GridEx IV event simulated a wide-scale physical- and cyber attack on the grid, with over 6,000 participants taking part.

## 3.8 California Response to Metcalf

Almost immediately after the Metcalf incident in April 2013, concerns were raised both in Sacramento and in Washington, DC, about future attacks by lawmakers who feared a repeat of a 9/11-scale homeland threat event.[27] For example, the author of SB 699 stated, "The security of our nation's infrastructure is of paramount importance."[28, 29] Similarly, a former vice president of a major California utility told a utility industry conference in November 2013 that the Metcalf incident was a sinister harbinger of worse to come. "These were not amateurs taking potshots," Mark Johnson, a former vice president for transmission operations at PG&E, warned the grid security conference. "My personal view is that this was a dress rehearsal" for future attacks.[30] Some months later and after the trade press broke the story, word of Metcalf and the alarm it was causing, mainstream news outlets got word with some repeating the dire warning with seeming little analysis or filter of skepticism.[31] As State Senate hearings concluded and facts were gathered, new California legislation began to coalesce on the issue. In 2014, the California Legislature passed and Governor Jerry Brown signed into law SB 699 which amended Section 364 of the Public Utilities Code.

[27] The concerns were compounded when it was reported that on August 26, 2014, PG&E reported a break-in at the same facility, with some $40,000 worth of equipment stolen. SED discovered the thieves had been on-site for over four hours. SED's investigation found gaps in training and security measures.
[28] California Senate Rules Committee, Bill Analysis of SB 699, 2014. Available for download at: http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0651-0700/sb_699_cfa_20140826_211913_sen_floor.html
[29] California Senator Jerry Hill August 29, 2014 News Release. Available for download at: http://sd13.senate.ca.gov/news/2014-08-29-hill-s-bill-heighten-electric-grid-security-sent-governor
[30] "'Military-Style' Raid on California Power Station Spooks U.S," By Shane Harris, Foreign Policy. December 27, 2013. http://foreignpolicy.com/2013/12/27/military-style-raid-on-california-power-station-spooks-u-s/
[31] "Assault on California Power Station Raises Alarm on Potential for Terrorism. April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid," by Rebecca Smith, *The Wall Street Journal*. February 5, 2014. https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879

Similar Federal legislation had been enacted by Congress in 2013, to address grid security at the transmission level. California legislators were able to look to the Federal example and in so doing, identified potential gaps in the new Federal legislation. Specifically, that grid assets subordinate to the transmission level had not been addressed. These distribution assets, which fall outside of Federal jurisdiction, but which are subject to Commission oversight, became a primary focus of the new law.

Public Utilities Code Section 364, as amended by the new law, requires the Commission to adopt standards for distribution facilities that provide for high quality, safe, and reliable service.[32] Additionally, Section 364 calls for actions to protect vulnerable electric distribution system assets from deliberate physical threats that could disrupt safe and reliable electric service. The statute also cites the need for appropriate planning in coordination with Federal, state, and local law enforcement authorities to minimize the chance of physical attacks and their potential impacts.[33]

Finally, the Legislature authorized the Commission to withhold certain records from the public where such information, if disclosed, would pose a security threat. This provision created for the Commission a new exemption that could be applied to the California Public Records Act requests for public access to documents.[34]

On June 11, 2015, the Commission issued Order Instituting Rulemaking (OIR) 15-06-009,[35] to establish policies, procedures, and rules to address physical security risks to electric distribution facilities. This active physical security proceeding, Phase 1 of the rulemaking, considers whether

[32] Pursuant to GOs 95, 128, 131-D, 165 through 167, and 174, Commission staff is routinely involved in the verification of the condition and operation of existing physical security protections. Additionally, D. 14-12-025, which created the utility RAMP (Risk Assessment and Mitigation Phase) process, requires all utilities to discuss safety and risk assessments in every rate case.

[33] Public Utilities Code Section 364, as amended, is expansive and the CPUC is addressing only physical security for electric facilities in this proceeding as a first phase. Section 364 also addresses disruption of essential public services such as safe drinking water, natural gas delivery, emergency response, or medical care.

[34] Public Utilities Code Section 364(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."

[35] CPUC, Order Instituting Rulemaking Regarding Policies, Procedures and Rules for Regulation of Physical Security for the Electric Supply Facilities of Electric Corporations, June 2015

new rules, standards, or modifications to existing policies or general orders are necessary to address the physical security risks to electric distributions facilities.

### 3.8.1 Other State Regulatory Policies and Practices Since 2014

A 2016 report by the National Council of State Legislators (NCSL) documents the fifty states' efforts in recent years to protect the electric grid.[36] It notes that the states are actively addressing threats to the nation's critical infrastructure including physical- and cyber security. Some states have sought to make the grid more resilient by diversifying energy production by such means as introducing microgrids to the distribution system. Several states have also supported smart grid technology which may increase grid resilience.[37] This section highlights a few of the more profile efforts of states that appear to show promise for their contributions to growing the existing body of knowledge surrounding state-level efforts to bolster grid security.

#### 3.8.1.1 Florida

An interesting example of state-level inquiry on grid security is the Florida Public Service Commission's 2014 publication, "Review of Physical Security Protection of Utility Substations and Control Centers",[38] which provided a comparative assessment of physical security approaches employed across Florida's four major investor-owned electric utilities.[39]

Findings from this effort include:

- Federal regulations such as NERC CIP requirements and actions by the U.S DHS, U.S. DOE, and other federal agencies have done much to safeguard the most critical bulk power system sector assets;

[36] Available for download at http://www.ncsl.org/Portals/1/Documents/energy/ENERGY_SECURITY_REPORT_FINAL_April2016.pdf

[37] National Council of State Legislatures, "State Efforts to Protect the Electric Grid" April 2016 Available for download at http://www.ncsl.org/Portals/1/Documents/energy/ENERGY_SECURITY_REPORT_FINAL_April2016.pdf

[38] Available for download at http://www.psc.state.fl.us/Files/PDF/Publications/Reports/General/Electricgas/Physical_Security_2014.pdf

[39] The four Florida IOUs are Duke Energy Florida, Florida Power & Light Company, Gulf Power Company, and Tampa Electric Company Florida Public Service Commission, *Review of Physical Security Protection of Utility Substations and Control Centers*, December 2014

- Extensive efforts and unknown levels of cost accompany utilities' compliance response to NERC reliability standards;
- Selecting and implementing prudent and proportional preparations against physical attack necessitates making value judgments;
- Continuous vigilance and frequent reassessment of risk analysis and threat analysis should be employed by utilities;
- The Florida Public Service Commission (FPSC) and Florida IOUs should work cooperatively to identify appropriate, prudent, and cost-effective levels of protection needed;
- Proposed utility physical security expenditures should be informed by focused risk assessments;
- Because costs must be weighed against potential benefits and perceived risks, utilities would benefit from guidance from the FPSC;
- Efforts by utilities to identify, disclose, and track physical security costs may be necessary, and a focused discussion of such expenditures in company filings and testimony would support appropriate spending.

#### 3.8.1.2 Texas

As of 2017, the State of Texas had in progress an initiative to develop a comprehensive physical- and cyber security outreach program for Texas investor- and publicly-owned electric utilities, and cooperatives. Led by the Public Utility Commission of Texas (PUCT), the program is a voluntary promotional campaign that enlists Texas utilities willing to assess corporate culture receptiveness to infrastructure protection efforts and identify areas for improvement.[40]

The objective of the Texas initiative is to:

- Recommend a collaborative framework for information sharing between the PUCT and Texas utilities during times of normal operations and emergency situations;
- Identify, evaluate, and report on existing utility practices for securing critical electric infrastructure and highlight best practices.

To date, although numerous states are actively engaged on electric utility physical security issues, no state-level regulations have yet been enacted.

[40] Public Utility Commission of Texas, *RFP to Develop A Comprehensive Cybersecurity and Physical Security Outreach Programs for Texas Electric Utilities, Electrical Cooperatives and Municipally Owned Electric Utilities*, March 2017.

### 3.8.2 Other Industry Initiatives

The Edison Electric Institute (EEI), a trade association for investor owned utilities across the nation, EEI promotes an approach to grid security to advance standards, public-private partnerships, and promotes strategies for preparation, prevention, and response.

Since 2014, Institute of Electronic and Electrical Engineers (IEEE) has been developing new guidelines on physical security, P1402 – Guide for Physical Security of Electric Power Substations. Expected to be issued in 2019, IEEE's guidance would offer recommendations on minimum requirements and practices for the physical security of electric power substations.

# 4 Distribution Asset Security and Resiliency in California

## 4.1 Distribution Assets Not Attractive High-value Targets

Despite the emphasis on preventing a repeat of a planned physical attack such as the Metcalf shooting, the vast majority of so-called physical security incidents on the distribution system consist of minor property crimes such as vandalism, copper theft, and trespassing. These are committed not by determined or organized attackers, but by opportunists.

In turn, utility supply yards are much more common locations for physical security incidents than distribution substations.[41] This is attributable to utilities' practice of procuring spare metal, particularly copper, in large bulk quantities to minimize cost. Gigantic copper spools weighing many tons are then typically stored in the open within utility supply yards. Metal thieves are known to trespass and cut out the spool a few pounds of copper, which may render the remaining copper worthless. Such copper spools, often easily visible, appear as more attractive targets for metal thieves than distribution assets, where any available copper would be more scarce, and difficult and dangerous to remove.

[41] It is typical that a supply yard is adjacent to a substation, but may be segregated by a wall or fence. These adjacent substations are typically larger-scale facilities consisting of transmission assets or mixed transmission-generation assets, and might range four to twenty times greater area of a typical residential-scale distribution substation.

Another insight gleaned from this proceeding is that the electric distribution system in general is not an attractive target for calculated sabotage due to its resiliency and resulting low impact value. In plotting their attacks, saboteurs usually seek publicity to advance their message; a distribution attack and outage would be unlikely to result in impacts that would generate the kind of significant media attention that organized malicious actors would seek.

The electric grid's existing resiliency condition is a result of the distribution system's deliberate redundancy by design. In a hypothetical case, say where a distribution substation transformer were to be targeted by multiple rounds of high-caliber ammunition resulting in a power outage (similar to a 2016 incident in Utah), distribution operators would typically be able to respond by way of remote grid-switching to bypass the affected substation. Meanwhile, the utility's reliability response team would work to rapidly dispatch replacement parts, including entire distribution transformers if needed, located at strategically-sited supply stations to quickly ensure that a facility is repaired and back on line, often within 24 hours.

# 5 Incident Reporting and Tracking Best Practices

*A round-up and comparison of information reporting, tracking, and trending activities among regulatory and industry organizations*

### 5.1.1 Commission-required Incident Reporting

The CPUC has no mechanism in place for electric utilities to specifically report physical security incidents at distribution facilities, and thus lacks a convenient means to track and trend such incidents.

The existing CPUC emergency incident reporting system,[42] may aid in identifying events that have physical security implications, but there is at present no aggregation of data reported through this system to monitor patterns or trends in physical security at the distribution level. It is also unclear of the level of resources the CPUC puts toward making use of its incident reports.

[42] Initial Notification Standard, required by GO 167, Section 10.4, specifies that utility incident reports are required to be filed with CPUC for incidents entailing property damage in excess of $10,000, significant media attention, or a power outage. Available for download here: http://www.cpuc.ca.gov/General.aspx?id=2721

Commission General Order 166 Standard 6 [43] stipulates that utilities must report within one hour of discovery, any major outage.[44] The Commission provides a GO 166 incident report summary in its annual report to the Legislature. CPUC Guidelines for electric utility emergency reporting were revised in 2012, and with oversight transferred from Energy Division to what is now the Safety and Enforcement Division (SED).[45]

Incident reports for 2015 and 2016 indicate a low number of physical security related incidents. In 2015, more than 300 incidents were reported to the Commission, with the majority associated with local outages. Only one percent, or three incidents, were linked to a physical security at a distribution asset. In 2016, there were over 150 incidents reported, but none were physical security related. Rather, weather, natural disasters, aging infrastructure, traffic accidents, utility contractors, tree trimming, and mylar balloons accounted for the reports.

### 5.1.2 U.S. Department of Energy - OE-417 Reporting

An existing mandatory U.S. DOE reporting system for emergency incidents and disturbances by public and private electric utilities, OE-417 - Electric Emergency Incident and Disturbance Report, appears to perform relatively well. The system is used by NERC to assess physical security trends for the bulk power system. Federal regulatory requirements specify that a Form OE-417 shall be logged by a utility within one hour of discovery of one or more of these qualifying events:

1. **Physical attack** that causes major interruptions or impacts to critical infrastructure facilities or to operations
2. Cyber event that causes interruptions of electrical system operations
3. Complete failure or shutdown of the transmission or distribution system
4. Electric system separation "Islanding"
5. Uncontrolled loss of 300 MW or more of firm load for more than 15 minutes from a single incident

[43] General Order 166, available for download here: http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M138/K073/138073150.pdf

[44] Defined as total loss of power impacting ten percent or more of a utility's customer base. This standard, which pertains to the three large electric investor owned utilities only, would trigger an incident report when there is a simultaneous, non-momentary interruption of service.

[45] CPUC Memo to rescind all prior versions of the *Guidelines for Notification of the CPUC Energy Division of Emergencies or Urgent Events in Electric Utility Systems, November 1, 2012.* Available for download at: ftp://ftp2.cpuc.ca.gov/PG&E20150130ResponseToA1312012Ruling/2012/11/SB_GT&S_0186388.pdf

6. Load shed of 100 MW or more implemented under emergency operational policy
7. System-wide voltage reductions of 3 percent or more
8. Public appeals for reduction in electrical usage
9. **Physical attack or vandalism** that could potentially impact electric power system adequacy or reliability
10. Cyber event that could potentially impact electric power system adequacy or vulnerability
11. Loss of electric service to more than 50,000 customers for one hour or more
12. Fuel supply emergencies that could impact power system adequacy or reliability

It is notable that the U.S. DOE OE-417 reporting program trigger criteria calls out physical security incidents as events needing to be reported within one hour of discovery by the utility.

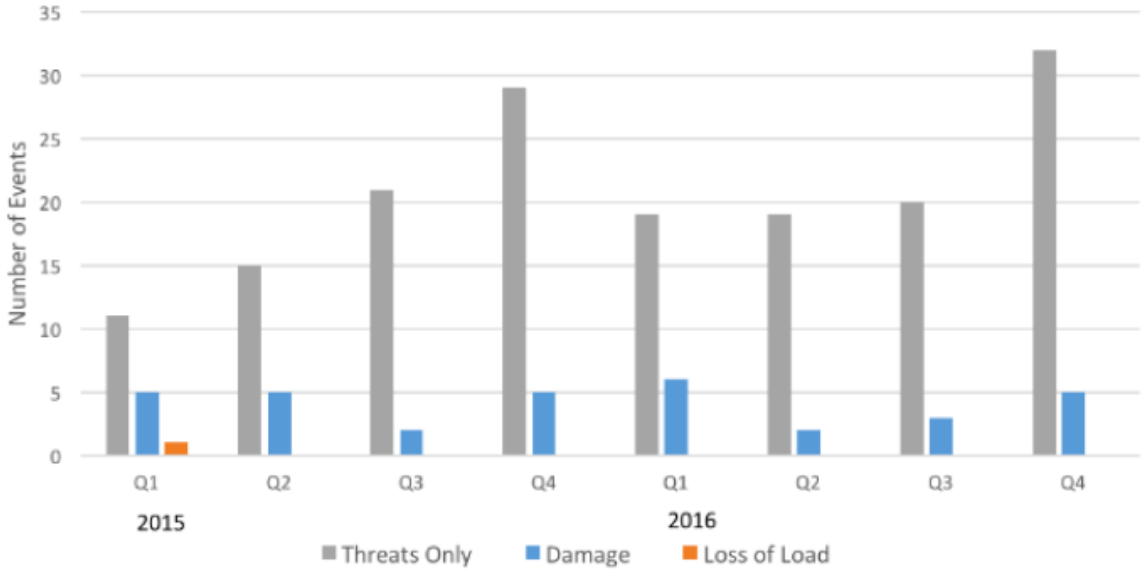
**Table 3. 2016 California Electric Physical and Cyber Events Reported in OE-417 reports**

| Month | Area Effected | Event Type | Demand Loss | Customers Affected |
|---|---|---|---|---|
| October | Mendicino Co. | Actual Physical Event | 0 | 0 |
| October | Imperial Co. | Vandalism | 0 | 0 |
| November | Stanislaus Co.<br>San Joaquin Co.<br>Alameda Co.<br>Tuolumne Co. | Cyber Attack | 0 | 0 |
| November | California | Vandalism | 0 | 0 |
| December | Riverside Co. | Cyber Event | 0 | 0 |

**Source:** FERC OE-417 reports

The OE-417 program has recorded few incidents of physical intrusions in California and nationally. NERC has concluded that the low numbers demonstrate that the electric industry's record of breaches is much lower than many other sectors (including government agencies). For 2017, NERC reported no major (Category 4 or 5) transmission outages. For 2015 and 2016, NERC reported one physical security incident that caused a loss of load (shown in **Figure 3**).

**Figure 3. Reportable Physical Security Events on Bulk Power System**




**Source:** U.S. DOE, OE-417 Report of Electric Disturbance Events

Despite its historic value as a reporting tool, the OE-417 system's value appears to be less than its full potential due to inaccurate and miscategorized incident reporting that goes unnoticed, ostensibly due to staff bandwidth limitations at regulatory agencies such as NERC. A recent example would be an April 21, 2017, fire[46] at a PG&E distribution substation at downtown San Francisco's western edge that resulted in an extended loss of power to some 90,000 accounts during peak business hours, and led the city and county of San Francisco to sue to recover losses.[47] The incident, which took out power at the CPUC and caused the agency to close for the business day, was reported by PG&E via OE-417 as a "systems operations" event.[48]

As it stands, the OE-417 reporting process provides some additional value for the Commission because these reports provide a secondary source of information on national trends, and vandalism incidents are not captured by CPUC emergency reporting. For this reason alone, staff recommends that jurisdictional utilities begin to copy the CPUC's Electric Safety and Reliability branch of SED and the Grid Planning and Reliability section of Energy Division anytime an OE-417 report is filed. Such filings will be treated in accord with prevailing State and Commission

[46] http://www.latimes.com/local/lanow/la-me-san-francisco-power-outage-20170421-story.html
[47] http://www.sfgate.com/bayarea/article/SF-to-dun-PG-E-for-187-000-in-losses-during-11125425.php
[48] https://www.oe.netl.doe.gov/oe417.aspx

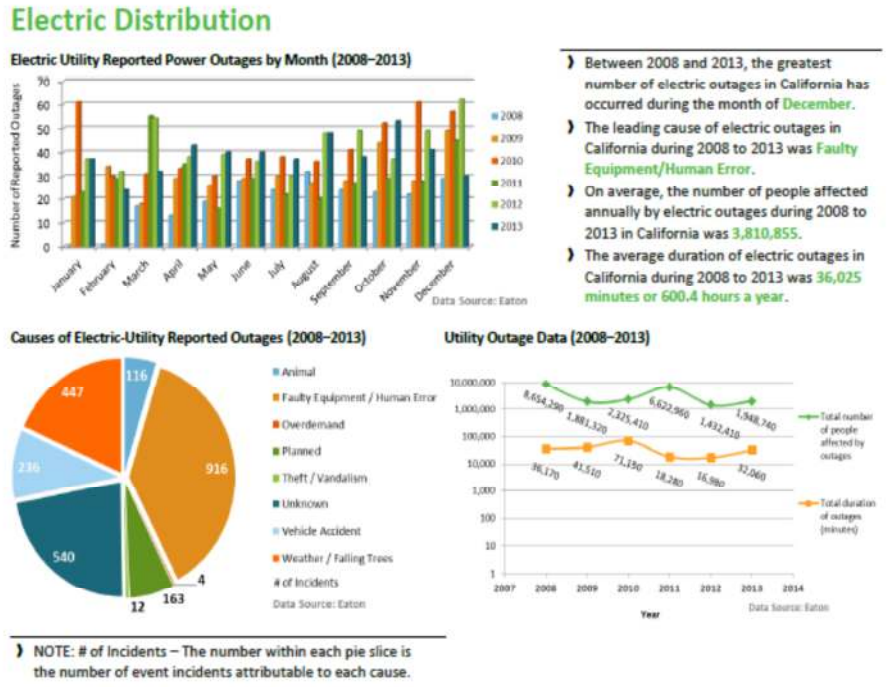
policy surrounding the safeguarding of sensitive information and exemptions from public disclosure.

### 5.1.3 U.S. Department of Energy – Other Data and Trending Resources

The U.S. DOE has published a series of State Energy Risk Assessments, with the intent of supporting public decisions about infrastructure, resiliency, and asset management. This is a joint effort with the National Association of Regulatory Commissions (NARUC), the National Association of State Energy Officials (NASEO), the National Conference of State Legislatures (NASL), and the National Governors Association (NGA).

California's *state and regional energy risk profile,* see **Figure 4**, below, presents risk factors typically attributed to California's energy infrastructure. NERC identifies faulty equipment/human error as California's primary cause of electric transmission outages. The risk profile also provides 2008-2013 data on transmission outages and causes. The data indicate that the *primary electric-outage risks are weather, natural disaster, or equipment failure.*

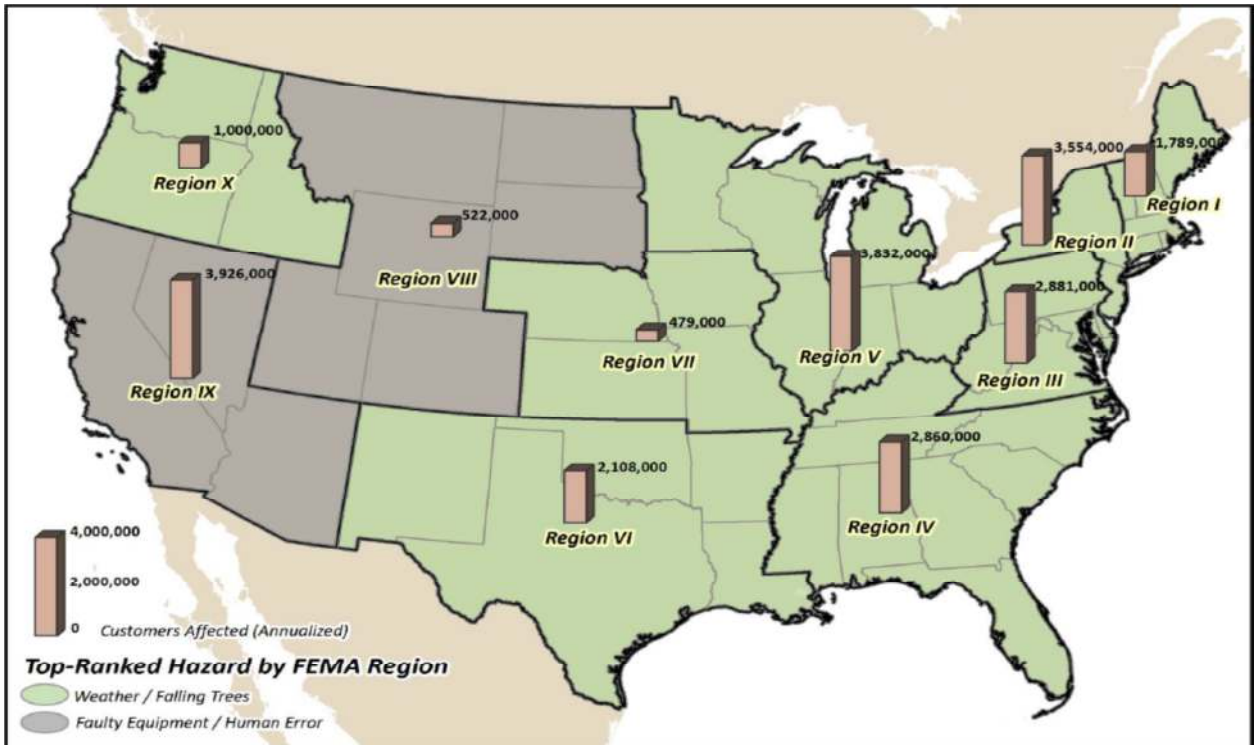
**Figure 4. State of California Electric Risk Profile**




**Source:** U.S. Department of Energy, Office of Electricity Delivery and Electric Reliability

As shown in **Figure 5**, below, U.S. DOE has also examined electric distribution system outages by region for the United States. It was found that the western region consisting of California, Nevada, and Arizona has the highest number of annual distribution outages (3,926,000) with the leading cause determined to be faulty equipment or human error.

**Figure 5. Electric Distribution Outages by FEMA Region by Argonne National Laboratory**




**Source:** U.S. DOE, National Electricity Emergency Response Capabilities, August 2016

To date, impact on grid reliability attributable to physical security incidents there has been rare and limited. Where such events have occurred, the number of customers impacted has been small and restoration of service has typically occurred within 24 hours. The fact that actual physical attacks comprise an insignificant share of electric system incidents has been cited in some news articles[49] as an indication that fears of malicious attacks are "overstated."

[49] A June 15, 2017, Bloomberg/BNA article asserted that many supposed reported physical security incidents were not sabotage with resulting loss of power or even vandalism, but rather pointed to petty theft. The problem stems, the article suggested, from confusion resulting from a 2010 change to OE-417 reporting requirements. Affected

However, the available documentation actually provides a sound basis for a public policy approach that *balances physical security efforts, where appropriate, with other utility efforts to ensure resilience of service.* Such an approach is valuable, not just for addressing physical security, but also for reducing impacts from weather events or the infamous "other" causes of system disturbances that more commonly impair system reliability.

### 5.1.4 Insurance Industry – National Insurance Crime Bureau

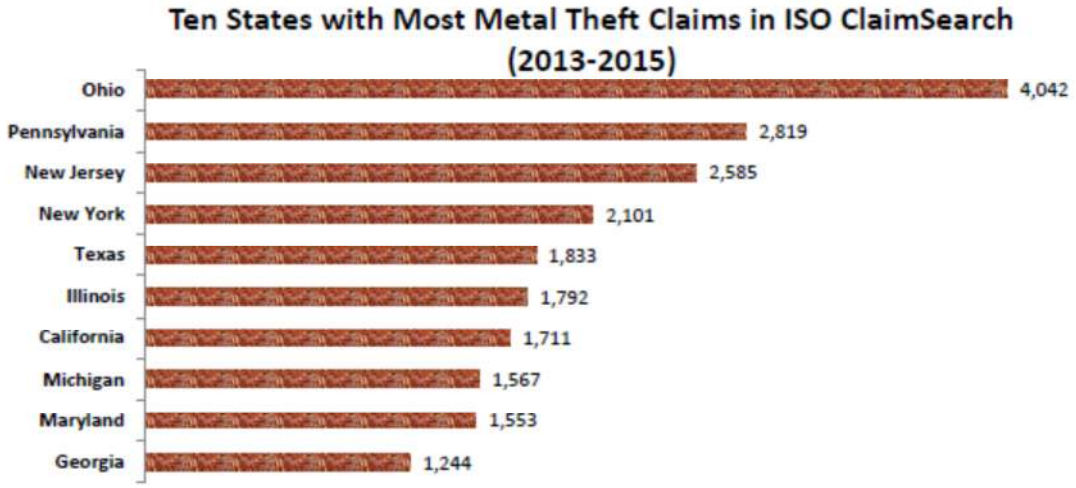
An effective example of private-industry methodology employed in recording and trending physical security incidents would be that of the National Insurance Crime Bureau (NICB). The NICB tracks those incidents linked to its 1,100 members and – using data analytics, investigations, and training -- represents insurers in cooperating with law enforcement and others to deter crime and insurance fraud.

NICB recognizes the value of information tracking and sharing, and its reporting system offers what appears to be the nation's best source for data on metal theft. The reporting system's success is contingent on member insurers comprehensively reporting all claims involving the theft of metal, typically copper. While NCIB does not, provide information specific to the electric industry, its data provides an accurate assessment of metal theft activity state by state, which would be representative of physical security issues linked to electric distribution facilities. This is because copper theft is perhaps the most common incident type at electric distribution facilities. As shown in **Figure 6** below, from 2013-2015 NICB data shows that California was among the top ten states in metal theft claims.

However, when adjusted for population size, California is not within the top ten states with metal theft problems. Compared with top ranked state Ohio at over 30 claims per 100,000 residents, California had just 4.4 claims, ranking it 41 of 50 states in metal theft claims on a per capita basis.

entities, it seems, are confused about when to file a report and how to file it, and so choose to err on the side of caution and thus over-report. *Malicious Attacks on Electric Grid Facilities Over-Reported,* Bloomberg Business News.

**Figure 6. 2013-2015 Ten States with Most Metal Theft Incidents**




**Source:** National Insurance Crime Bureau, Metal Theft Claims Down 8% Since 2012, September 9, 2015

The insurance industry model for tracking physical security events holds several advantages over the existing electric industry approach. For one, this tracking function is performed by an organization that has information management and data analytics as its primary mission and possess the resources to provide meaningful, accurate information to its members. This information generated by the insurance industry has superior granularity and quality assurance than the reporting systems employed by the CPUC or U.S. DOE.

# 6 Exchange of and Access to Highly Confidential and Sensitive Information

Information sharing can reliably be counted on as a high profile issue in Commission matters, and this proceeding is shaping up to be no different. The crux of the issue here appears to be How to balance disparate and well-intended, but seemingly conflicting goals surrounding the Commission's responsibility to protect the public and the Commission's responsibility to provide the public with access to information?

The first goal would be the seemingly legitimate limitation of information dissemination to safeguard against data unintentionally falling into the wrong hands. The conflicting second goal would be the transparency and openness in government. A third consideration and priority

would be the Commission's ability to have rapid and unfettered access to the full set of facts and data surrounding a utility issue or impending crisis. Thus, the Commission, its staff, and regulated entities recognize that an effective physical security program will need to facilitate the quick and easy exchange of vital information among participants.

Further complicating matters are legitimate concerns surrounding cyber security. As a result of a series of high-profile identity theft and ransomware incidents in 2016 and 2017, it is now well recognized at both the security-expert and consumer levels that remote exchange of digital information is highly vulnerable to cyber threats.

The Commission relies heavily on the data request process as a primary means for staff to carry out its regulatory duties. For the vast majority of cases, CPUC staff is able to obtain at least partial fulfillment of the requested data, which may or not be confidential, in electronic format[50] and within two to three weeks without the need to meet with or hold a complex conversation with IOU staff.

Still, there are cases in which a standard data request to a utility may be a poor fit given the sensitivity of the information requested. The Legislature within SB 699, granted the Commission authority to withhold public disclosure of certain information with the intent of preventing homeland security-scale secrets from being exploited by malicious actors. As part of this proceeding, SED and utility staff have cooperated to try to determine new proposed thresholds and definitions for *highly confidential* and *sensitive* information, categories more restrictive and unusual than the relatively common *confidential*[51] information category described in PU Code Section 583. Additionally, the proceeding has attempted to determine if these new categories of information can be exchanged and accessed by electronic means. This chapter presents background, existing status, and a look at what may lie ahead on the Commission's evolving treatment of sensitive information.

[50] The CPUC has various electronic data transfer tools with varying degrees of perceived cyber security.

[51] Broad rules exist for restricting public disclosure of utility records and designating them as confidential, with private consumer information and use data (GO 77-M) being two of the more common items. Probably more routine in their application to data submitted to the Commission, is the utilities' use of GO 66-C, which among other things, broadly protects "Reports, records, and information requested or required by the Commission that, if revealed, would place the regulated company at an unfair business disadvantage."

## 6.1 Existing Federal Standards and FERC Protocols

Existing standards for the sharing of information on critical electric infrastructure by the U.S. electric industry has been shaped by Federal rules, which define critical electric infrastructure information that warrants secure management by all parties.

Treatment of sensitive information regarding critical energy infrastructure has been a Federal priority issue since 9/11, with FERC adoption of PL02-1000 in October 2001. FERC has since actively updated its information sharing policies. In 2003, FERC adopted Order No. 630, which included a definition of *Critical Energy/Electric Infrastructure Information* (CEII). CEII-designated information is treated by FERC as privileged and confidential, not subject to the Freedom of Information Act (FOIA). Information categorized as CEII is limited and includes specific engineering, security, and design details about existing or proposed critical infrastructure. Most recently, in 2016, FERC adopted Order No. 833, which added Section 215A to the Federal Power Act to address security and resilience of energy infrastructure.[52]

Access to CEII is restricted because it conveys strategic information beyond the location of critical infrastructure and could be useful to a person planning an attack on critical infrastructure. Further details of FERC's approach to information access, and definitions employed for information sharing policies, may be found in **Appendix 2**.

## 6.2 Commission Policies and Recent Decisions on Information Security

The issue of confidential information exchange between utilities and the Commission dates back at least 40 years and is addressed in the PU Code and Commission General Orders. Public Utilities Code Section 583 sets forth a process for dealing with claims of confidentiality but does

[52] The definition of Critical Energy/Electric Infrastructure Information is codified in Section 388.113(c), Chapter I, Title 18, Code of Federal Regulations, which governs the procedures for submitting, designating, handling, sharing and disseminating CEII submitted to or generated by FERC. Critical Electric Infrastructure Information is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3), and shall not be made available by any Federal, State, political subdivision or tribal authority pursuant to any Federal, State, political subdivision or tribal law requiring public disclosure of information or records pursuant to section 215A(d)(1)(A) and (B) of the Federal Power Act.

not contain any substantive rules on what is and is not appropriate for protection.[53] GO 66-C, first adopted in 1974, and updated in 1982 (and superseded by GO 66-D in 2018) identifies procedures for the treatment of public records at the Commission. GO 66-C identified all Commission records as public unless they fall within a short list of exemptions.

## 6.3 GO 66-D and Confidential Matrices

Under Rulemaking (R.) 14-11-001, now in progress, the Commission has been examining public access to public records with the goal of providing clarity on when information should be considered confidential. On September 28, 2017, the Commission completed the first of two phases of the rulemaking by adopting GO 66-D and new administrative processes for submission and release of potentially confidential information.[54] GO 66-D replaced GO 66-C, and became effective in January 2018. GO 66-D specifies a process for:

1. Regulated entities and the public to submit information with a claim of confidentiality
2. The public to submit requests for information per the California Public Records Act; and
3. The Commission to determine whether a claim of confidentiality is lawful and appropriate

In the second phase of the confidentiality rulemaking, the Commission expects to address a significant change included in GO 66-D regarding the concept of "Confidential Matrices." The term describes a Commission determination that specific categories of information are confidential per Section 3.4 of GO 66-D. The determination would be made prior to submission to the CPUC of such information, and would apply broadly to a category of documents. If information has been submitted in compliance with a specific confidential matrix, it would not be released per a California Public Records Act request absent an Order of the Commission. This would be applicable to physical security information from the utilities.

The utilities endorse a confidential matrix consistent with FERC protocols that uses the CEII designation for a class of information relating to critical energy infrastructure physical- and cyber security sensitive information. It also cites a category of information defined in FERC

[53] D.06-06-066 at 27, as modified by D.07-05-032.
[54] CPUC Decision 16-08-024, September 28, 2017.

regulation, *Sensitive Security Information* (SSI).[55] The physical security rulemaking is somewhat intertwined with the confidentiality rulemaking as development of a confidential matrix for the electric industry would determine when information is to be categorized as CEII and SSI, and would impact how physical security information is to be shared between electric utilities and the Commission.

SED staff continue to closely monitor the R.14-11-001 proceeding. While the CEII and SSI designations are consistent with FERC protocols, the Commission would need to define the type of information that qualifies for such designation and how the Commission would vet any proposed request for designation. It is expected that the confidentiality proceeding will conclude in early 2018, approximately the same time that the current Phase 1 of the physical security rulemaking would be coming to a close. SED staff believes that the confidential matrix proposed by the electric utilities would be adequate and generally consistent with the outcome sought by the physical security proceeding.

**Table 4. Joint Energy Utilities Working Group Matrix of Confidential Materials Relevant to Physical Security of Electric Distribution Systems**

| Type of Information | Examples | Justification |
|---|---|---|
| **Personally identifiable information (PII) of regulated entity Customers** | Social Security Numbers | |
| **Personally Identifiable Information of Employees or Contractors** | Names, home and email addresses, telephone numbers | |
| **Investigations of Regulated Entities** | Orders Instituting Investigation, Audits | |

[55] As part of the confidentiality proceeding, the Commission requested that parties submit proposals for confidential matrices. Working groups were formed for various utility industries regulated by the Commission for the purpose of developing matrices applicable to their industry. California electric utilities formed a Joint Energy Utilities Working Group and jointly filed a proposed matrix on October 3, 2017 that identifies specific categories of information proposed as being exempt from PRA requests.

| | | |
|---|---|---|
| **Corporate, Financial and Proprietary Records** | Tax Returns, Board Minutes, Non-public Company Financial Information | |
| **Critical Energy Infrastructure and Physical- and Cyber Security Sensitive Information** | ▪ Critical Energy/Electric Infrastructure Information (CEII)[56]<br>▪ Sensitive Security Information[57] (SSI)<br>▪ NERC Critical Infrastructure Protection (CIP) Information<br>▪ Physical facility information<br>▪ Electric Facility Information | Protected under Gov't Code §§6254€; 6 USC §131(5); 68 Fed. Reg. 9857 (DOE Mar 3 2003) (final rule); Cal. Pub. Util. Code §364(d).<br><br>18 CFR 388.113©; FERC Orders 630, 643, 649, 662, 683, and 702 (defining CEII); 68 Fed. Reg. 9862 (DOE Mar 3 2003) (final rule)<br><br>Critical Infrastructure Information[58] Gov't Code 6254€, (k), (ab) |

Source: Energy utility working group filing in R.14-11-001[59]

## 6.1 Protected Critical Infrastructure Information (PCII) Platform

The Critical Infrastructure Information Act of 2002 established the Protected Critical Infrastructure Information (PCII) program[60] as a secure sensitive information portal for data on the nation's infrastructure. The PCII platform is intended as an information depository and -

[56] 18 CFR §388.113© defines "critical energy infrastructure information" as "specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure" that

I. Relates details about the production, generation transportation, transmission, or distribution of energy,
II. Could be useful to a person in planning an attack on critical infrastructure,
III. Is exempt from mandatory disclosure under the Freedom of Information act, 5 USC 552 and
IV. Do not simply give the general location of the critical infrastructure.

[57] 49 CFR 1520.5(a) defines "sensitive security information" as:
Information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would –

1. Constitute an unwarranted invasion of privacy 9including but not limited to information contained in any personnel, medical, or similar file);
2. Reveal trade secrets or privileged or confidential information obtained from any person; or
3. Be detrimental to the security of transportation

[58] Defined in 6 USC 131(3).

[59] Southern California Edison, Proposed Matrix of the Joint Energy Utilities Working Group Pursuant to Assigned Commissioner's Ruling Regarding Phase 2B, October 3, 2017.

[60] More at: https://www.dhs.gov/pcii-program

sharing resource to advance homeland security goals by lowering barriers to and increasing privacy in the exchange of sensitive information between U.S. DHS and entities in allied fields.

All Information granted PCII status is automatically exempt from compliance with Freedom of Information Act (FOIA) requests or requests from any public entity. Similarly, PCII data are exempt from disclosure in civil litigation and from regulatory use purposes.

Clearance for PCII access requires rigorous background screening. Eligible staff or contractors of Federal, state, local, tribal, or territorial governments must complete PCII training; be employed in homeland security duties; and have demonstrated a valid need for access to particular information.

In California, one example of the possible application of PCII might be a utility or operator sharing details of electric grid and generation assets that would allow DHS staff to consider these facilities within the overall and emerging threat landscapes. A second example might be for Commission staff to retrieve sensitive information in real-time and via a secure platform from utilities regarding their electric assets. The existing regulatory-use exemption tied to PCII data may complicate the Commission's reliance of the platform for routine business, but the use of PCII merits further consideration, particular in the event of an emergency.

# 7 Utility General Rate Cases Informing Physical Security Efforts

One expected outcome of the Physical Security rulemaking is a new process for utilities (both investor owned and publicly owned) to better identify assets that may be vulnerable to attacks or disruptions that pose a substantive threat to physical security or cause service disruptions and devise plans for mitigating the risks.

Eventually, for CPUC jurisdictional utilities, the costs of such preventive measures – whether in the form of "hardening" assets against attack, or ensuring that any disruptions to service are minimized by bolstering the resiliency of the system – would be accounted for in General Rate Case applications. Such costs would be separate from and additional to those incurred to meet federal requirements for protecting Critical Infrastructure; in particular, the CIP-014 protocols that are overseen by the NERC and subject to rulemaking by the FERC.

As a result of the physical security rulemaking, and as an outcome of the Safety Model Assessment Proceeding (S-MAP) process and Risk Mitigation Assessment Phase (RAMP) for identifying and mitigating safety risks in GRCs, the Commission anticipates greater transparency about what utilities are doing to enhance physical security and at what cost to ratepayers.

An additional expected outcome would be a greater consistency in the reporting of plans and expenditures among the utilities whose quality and quantity of information they provide to the CPUC about physical security spending now varies widely.

The following narrative briefly describes how physical security has been documented in the most recent GRCs.

**Pacific Gas and Electric Company**

Despite the enhanced physical security upgrade program announced by PG&E in the wake of the Metcalf incident, the IOU did not provide much information in its most recent GRC covering the 2016-2018 period (A.15-09-001). In its GRC testimony, PG&E noted that costs associated with physical security at distribution substations are bundled together in Major Work Category 58, via four subprograms covering safety, security, fire protection, and seismic enhancements.

"Expenditures include the replacements or upgrades of substation fences, security cameras and card readers, fire suppression systems and seismic retrofits to control buildings." At the time of its filing, PG&E did not project any expenditures to meet future requirements under SB 699/R.15-06-009, and it did not plan to recover any costs during this rate case cycle.

That said, the utility documented over $1 million in distribution substation security measures in 2014, with a varied projection of expenditures through 2019 approaching $6 million in total:

**Table 5. ($000) PG&E Distribution Substation Security Spending 2014-2019; PG&E, pp. 12-27**

| Substation | 2014 (actual) | 2015 (forecast) | 2016 | 2017 | 2018 | 2019 | Total |
|---|---|---|---|---|---|---|---|
| Security | $1,070 | $461 | $364 | $1,300 | $1,300 | $1,300 | **$5,795** |

The settlement of the PG&E GRC approved by the Commission in D.17-05-013 did not alter PG&E's forecast spending on substation security. In November 2017, the utility will file a first-of-its-kind RAMP for the next GRC cycle, in which it is expected to provide more details on risks and mitigations associated with both physical- and cyber security.

**Southern California Edison**

In contrast to PG&E, SCE provided a great deal of information about its physical security efforts, but at part of testimony on Corporate Security (SCE-7, Vol. 5). Its documentation was largely about expenditures and projects to comply with the strengthening of CIP-014 standards at the federal level, with no detailed information about distribution-level asset security. However, the utility's testimony devoted to transmission and distribution substation construction (SCE-02, Vol. 6) provided a high level of expenditures for substation physical security during the GRC period 2016-2020, with a breakout for costs that are CPUC jurisdictional amounting to over $49.5 million for the forecast period.

SCE noted that it has 188 transmission substations and 677 distribution-level substations. Many substations reduce voltage from transmission level to distribution level voltages, so are dual jurisdictional.

**Table 6. ($000) Substation Construction and Maintenance, Total and CPUC Jurisdictional; SCE-06, Vol. 6, p.2**

| | **2016** | **2017** | **2018** | **2019** | **2020** | **Total** |
|---|---|---|---|---|---|---|
| Total Substation Physical Security | $22,341 | $51,617 | $25,641 | $22,404 | $23,877 | $145,880 |
| CPUC Jurisdictional | **$10,040** | **$12,226** | **$9,403** | **$8,798** | **$9,077** | **$49,544** |

Within its substation physical security program, there are three categories of spending: Copper theft mitigation program, CIP-14 compliance and lower-tier in terms of potential impacts on the system if a physical attack or breach occurs. SCE described physical upgrades for CIP-14 compliance, including: improvements to walls, reinforcement of gates, concealing key assets,

and improved cameras, alarms and lighting. The utility projected full upgrades for about 7 substations per year for CIP-14 program and as many as 29 per year for the lower-tier substations. The copper theft mitigation program largely entails additional fencing and lighting where needed.

**Table 7. ($000) SCE Substation Physical Security Enhancement; SCE-02, Vol. 6, p. 46**

| Program | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | Total |
|---|---|---|---|---|---|---|---|---|
| Copper Theft | N/A | $3,330 | $8,151 | $8,321 | $8,530 | $8,798 | $9,077 | $46,207 |
| Tier 1 CIP-014 | $10,861 | $14,344 | $14,190 | $42,550 | $9,052 | N/A | N/A | $90.997 |
| Tier 2-4 | N/A | N/A | N/A | $746 | $8,059 | $13,606 | $14,800 | $37,211 |
| **Total** | **$10,861** | **$17,674** | **$22,341** | **$51,618** | **$25,640** | **$22,404** | **$23,877** | **$174,414** |

*Note: Except for expenditures under the Copper Theft prevention program, these figures relate mainly to FERC jurisdictional transmission assets*

**San Diego Gas & Electric Company**

SDG&E's most recent GRC was for TY 2016 (A.14-11-003). Unlike SCE, the utility's testimony does not provide much detail on physical security expenditures to comply with federal CIP-014, noting only that such expenditures would fall under Infrastructure Integrity, Physical Security and Environmental costs. For the three-year GRC period, SDG&E projected a total $100.5m for capital for this category, and an O&M (operations and maintenance) budget of $11.22 million for TY2016 (future year O&M spending was established under the attrition year adjustments approved in the final GRC decision D.16-06-054).

For its GRC, SDG&E documented a steady-state physical security budget of $834,000 per year in 2014-2016, essentially the same as actual 2013 spending. The cost justification was based on increase compliance for critical infrastructure at 59 substations and to prevent copper theft and sabotage, according to SDG&E (SDG&E-09, p. 101). Among security measures in the program: video surveillance, nighttime illumination, access control door card readers, perimeter microwave intrusion detection and alarms. Security systems would be installed at all 230 KV cable locations.

In its more recent 2019 GRC filing made in October 2017, the Sempra Utilities did not provide a budget for risk assessment for physical security of electric assets of SDG&E. However, some categories of risk mitigation would entail spending for physical security. For example, to reduce the “workplace violence” risk, SDG&E requests about $3.4 million in physical security upgrades in 2019, and approximately $340,000 for physical security awareness training.

# 8 CONCLUSIONS

It appears that the North American electric industry is in intermediate stages of fully harnessing the potential of security technologies and staff expertise, and integrating security and risk assessment values into the utility culture such that utility physical security ultimately is prioritized on par with safety and reliability.

With advances in and lower costs of monitoring equipment, IOU security operations centers are extending the reach and capability of their physical security staff. In the coming years, IOUs will continue to ramp-up hiring of security experts who possess the knowledge necessary to adapt physical security methodology to IOU culture and needs. These experts would be able to bring on line and integrate into their IOU's retrievable recordkeeping systems the ability to optimally cull, trend, and process the vast quantities of data brought about by recent advances in technology. IOUs are growing their security data collection, trending, and forecasting capabilities as an emerging new field of expertise within the electric utilities. Such staff expertise and specialization may better ensure that a utility's many divisions are sharing data points on emerging threats so as to inform a full and accurate grid security assessment.

California's electric IOUs are well ahead of many of their peer organizations in North America and are serving as physical security innovators within the electric industry. Driven in part by NERC CIP-014 regulations, California IOUs have upgraded security operations centers and have "hardened" select transmission and distribution facilities (incorporating security upgrades that include perimeter fencing, electronic monitoring equipment, and improved access control).

The IOUs are also continually testing new equipment to assess its potential and cost-to-benefit tradeoff. Still, while California IOUs have demonstrated they are well ahead of many of their peer utilities, they have some ways to go to attain their full physical security potential and competency.

## 8.1 Room for Improvement in Demonstrating Adequacy and Competency

As stated in the FERC order that led to CIP-014, it is essential that electric utilities "demonstrate that they have taken steps to address physical security risks and vulnerabilities."[61]

IOU physical security efforts, staffing, and expertise appear to rely in large part on veterans of the military and law enforcement. While these expert backgrounds provide valuable rigor and standardization to physical security efforts, at times the tightlipped security culture they bring to the hinders the Commission's efforts to ensure transparency. Uneven rapport and uneven resources put toward rapport building among the physical security staff at the three IOUs with SED was evident in in 2017 in the course of carrying out routine regulatory oversight functions.

The culture difference that exists between regulatory and martial professions that is now being felt within the halls of the utilities and the Commission will need to be bridged and crossed to facilitate appropriate oversight of the physical (and cyber) security activities of jurisdictional utilities. SED staff encourage the IOUs to provide a signal of their commitment to reform disclosure and information sharing.

In addition, SED staff have witnessed varying degrees of preparedness, cooperation, and openness in interactions with IOU staff overseeing threat and security efforts. There remain issues with IOU staff turnover, evidence of disorganization when there is a handoff of roles and responsibilities to newly assigned IOU staff, and when the left and right hands of a utility organization function seemingly without knowledge of the other's actions.

Given the sizable expenditures put toward physical security as described above, there is an obligation for the utilities to better demonstrate and convey how these monies are being appropriately programmed, how grid assets are being adequately protected, and how risk is being managed in a responsible and optimal manner.

For now, as a result of this proceeding, the IOUs and SED staff appear to be in agreement that a balance can be found between safeguarding necessary classified-level information and ensuring that regulators are able to assess adequacy and competency without undue barriers and delays.

[61] 146 FERC 61.166. *Reliability Standards for Physical Security Measures*, March 7, 2014.

The Joint Utility Proposal – in whatever final form it may take – provides a potential solution to this need, and provides the Commission an initial platform for applying a standardized assessment and mitigation approach that represents a good beginning point.

# 9 RECOMMENDATIONS

## 9.1 SED STAFF RECOMMENDATION ON INCIDENT REPORTING

The CPUC has in place procedures for incident reporting by the utilities, but which do not specify physical security incidents.

Chapter 5 describes an existing mandatory U.S. DOE reporting system for emergency incidents associated with electric utility assets, and which includes physical security lapses and vandalism incidents. These OE-417 reports are prepared by California's investor- and publicly-owned utilities in accord with NERC rules and are submitted to NERC and WECC.

The OE-417 reporting provides some additional value for the Commission because these reports provide a secondary source of information about national trends, and the inclusion of vandalism incidents is something not captured under CPUC emergency reporting. For this reason alone, *staff recommends that jurisdictional utilities copy the CPUC's Electric Safety and Reliability branch of SED and the Grid Planning and Reliability section of Energy Division anytime an OE-417 report is filed.*

SED, which is the delegated lead within the Commission for CPUC incident reports, could then work to internally make improvements to make CPUC reports and OE-417 reports records more searchable, actionable, and adept to trend analysis.

## 9.2 Policy Recommendations and Advisable General Strategies

### 9.2.1 Pursue Information-sharing Partnerships that Offer Low Barriers and High Returns

In the realm of providing for physical security of critical assets, it is vital to follow the example among federal law enforcement and intelligence agencies to proactively cooperate to exchange leads, information, and best practices. For the purposes of state-level security oversight efforts, we provide here examples of utility partnerships that can support this goal.

### 9.2.2 Interagency Partnership Efforts

California's electric grid security concerns are ones shaped by factors perpetually subject to change. Fortunately, the State's industry and regulators are among the nation's most capable experts at responding and adapting to new threats, hazards, and vulnerabilities as they emerge.

In the post-9/11 environment, and in the wake of the U.S. intelligence, law enforcement, and customs agencies' communication shortcomings that led to establishing the Department of Homeland Security (U.S. DHS), collaboration among critical entities has become such an indispensable strategy that its importance is now largely understood by Americans even outside the security profession.

Similarly, collaboration and information sharing have become a new urgency for the U.S. electric industry in the years following the Metcalf incident. Increasingly, the formation of effective and innovative partnerships that bridge industry, regulators, emergency management, third-party, and law enforcement expertise are being looked to as a high-return, low-barrier-to-entry physical security strategy.

While still in progress, the physical security Phase 1 rulemaking appears to demonstrate how California can quickly assemble a functioning electric industry partnership bridging geography and other differences at nominal cost to locate solutions that make the grid and the public safer.

There is reason to believe that the Commission – with the aid and cooperation of its partners – can repeat this outcome to continue in a leadership role in the pursuit of establishing permanent physical security partnerships. Indeed, as a California public institution, the Commission is unique in its significant resources, strong voice, reputation for positive progress, and regulatory power available to forge new public-private working alliances to advance the security of those industries it oversees.

There is precedent for the Safety and Enforcement Division to enter into interagency partnerships via memoranda-of-understanding with sister state agencies, including Cal-OES).[62]

This MOU relationship allows for joint sharing of information and a seat at the table within response efforts to emergency situations. There is potential to expand such MOU relationships to other key agencies in the physical- and cyber security realm, including the network of law-enforcement intelligence fusion centers.

To this end, SED recommends that the informal Utility Physical Security Working Group formed for this proceeding (and which formulated the Joint Utility Proposal) continue to convene and be encouraged to engage with the Commission and its staff. SED should forge stronger ties and rapport with key physical security partners such as Cal-OES, and U.S. DHS, with participation by the utilities and their working group. Such collaborative efforts could help determine information-sharing platform standards, along with proactive exchange of tools and best practices to ensure that appropriate information on actionable threats, hazards, and vulnerabilities is available to relevant parties.

### 9.2.3 Joint Utility Partnership Efforts

As part of their compliance efforts to meet the challenges of critical infrastructure protections, utilities across the nation have joined in various task forces and working groups to share information and best practices. One example would be the member electric utilities within WECC's utility working group.

[62] Available for download at: http://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/Safety/Cal-OES%20CPUC%20MOU%20FINAL%20SIGNED(1).pdf

Utilities have actively entered into mutual aid agreements to dispatch staff and resources outside of their service territories in the event of an emergency or catastrophic event affecting an allied member utility. Such agreements, which commit to deploying a surge of qualified technicians to an impacted area, allow for shorter response times and more thorough restoration of electric service. Whether for hurricanes, wildfires, or earthquakes, the nation's utilities have demonstrated a reliable record of coming to the aid of one another and American energy consumers under difficult and trying circumstances.

In recent years, this asset sharing approach has also been put to use as a kind of preventative measure, one example being a joint utility lending program for replacement distribution transformer equipment that can be rapidly dispatched to respond to an emergency outage in the event electric operations equipment is compromised. Such lending programs work as cooperative resource leveraging to boost utility deployment capabilities at reduced cost compared to each utility having to store maintain vast inventories of idle parts to hold in reserve and at the ready.

Such agreements might also be valuable for other types of utility equipment, and California electric utilities should focus additional attention to and demonstrate competency with modeling and *robust assessment of supply chain vulnerabilities* and inter-utility agreements to create a shared stockpile of certain scarce and high-priority equipment.

Given the inherent interdependencies associated with California's electric grid, actors responsible for its physical security should share resources and data to improve monitoring of operations that span utility territories. Working collaboratively, California utilities should identify and map nodes, choke points, and other key points along the edges of their service territories. Such practices hold potential to improve the ability to monitor statewide performance of the distribution system's various components, and to forecast and model impacts on these interdependent systems.

California utilities should consider the value of, and report back to the Commission with an opinion on, available tools such as the Environment for Analysis of Geo-Located Energy

Information (EAGLE-I) managed by the U.S. DOE, which inputs data directly from energy sector partners, performs big data analysis, and shares situational awareness data.

California utilities should consider the value of, and report back to the Commission with an opinion on, U.S. DOE's new information classification system, "Critical Electric Infrastructure Information" (CEII) that facilitates voluntary sharing of critical electric infrastructure information between federal, state, and local government, and utilities.

### 9.2.4 Protect by Enhancing Preparedness and Prediction Capacity

Similarly, California electric utilities, working with appropriate public agencies, should plan and practice response procedures for incidents targeting sector interdependencies and entailing coordination across entities or business lines.

- IOUs should include physical security incidents as components to be addressed within their emergency preparedness plans and drills.
- California electric utilities' regular planning and preparation for major outage incidents should incorporate physical security strategies.
- California electric utilities should be proactive to incorporate the latest modeling and quantitative risk analysis tools, methodologies, and expertise to record, categorize, and trend incidents to more thoroughly expose threats to the electric grid.
- California electric utilities should offer an opinion to the Commission on whether the U.S. DHS Security Regional Resiliency Assessment Program could have value in protecting California's distribution systems.[63]
- Given the strong evidence[64] which suggests that California's primary risk of electric outages can be attributed to weather, natural disaster, or equipment failure, any rigorous distribution system resiliency plan would need to include strategies for addressing these three factors, which fall well outside of physical security parameters.

[63] This program consists of DHS conducting a regional analysis of critical infrastructure to address infrastructure resilience issues that could have regional or national consequences.
[64] U.S. DOE, California state energy risk profile.

### 9.2.5 Apply Technology, Innovation, and Investment to Bolster Grid Resiliency

California's electric utilities should improve their ability to monitor the grid's operating conditions and enhance their ability to pinpoint a problem and reroute power around any affected area.

California utilities should leverage grid modernization technologies including smart meters. Today's grid sensors are capable of detecting and monitoring grid anomalies to enable full integration of networked distributed energy resources. Deploying such devices would enable utilities to more quickly and precisely locate where actions and supplies are needed when incidents occur. Expanded networks of sensors hold promise for improving data transfer of diagnostics that monitor grid operations, improving response time and breadth. There is also great potential for improving reliability by way of automated responses to events. By beginning now, within a generation's time we may have an electric grid that is more flexible and agile, and would accommodate new plug-and-play technologies mindful of maximizing security and resilience. Such a future grid would be capable of restoring power with minimal intervention, ensuring that power flow can be quickly reconfigured, frequencies can be stabilized, and voltages can be controlled. And with utilities' improved outage response efficacy, there would be sizable operational cost savings.

### 9.2.6 Weave Physical Security Principles into Utility Corporate Culture and Embrace Consistency Statewide

To ensure more consistent physical security initiatives among the utilities, their security and response teams should identify those best practices which provide actionable steps for utilities to avert and respond to outage incidents.

Should the Commission find that statewide consistency among utilities' preparation for and response to outage incidents is desirable, utilities should demonstrate their coordination on mitigation, response, and recovery efforts for a range of threats. In the vein of the joint utility partnership opportunities described above, California electric corporations should form alliances to provide mutual aid and sharing of response resources when one or more members is in need of assistance due to an emergency incident.

### 9.2.7 Capital Projects in the Pipeline

California electric utilities should be mindful of opportunities for grid architecture improvements when considering new security and resilience measures. After all, one desired outcome of California's smart grid initiative would be to enhance security and resilience.

Common approaches for incorporating physical security into transmission include: hardening of facilities, Protection in Depth (PID), and Crime Prevention Through Environmental Design (CPTED). Because practical and more economical physical security opportunities abound when projects are conceived with these measures in mind, there should be an emphasis on incorporating them into any substation from the time of its inception. Moreover, it should be the established policy of California and its electric facilities that these measures be considered and incorporated where practicable and appropriate within newly-constructed substations or substations that undergo a significant rehabilitation.

Similarly, each time a utility restores power after a major outage, an opportunity exists for the recovery effort to extend beyond mere in kind replacement. When rebuilding, opportunities often exist for improvements to the electric grid that go beyond mere restoration of prior infrastructure. Acting on such opportunities should be embraced by the utilities and encouraged by the CPUC.

###

# APPENDIX 1 | CIP-014 NERC GUIDELINES | PHYSICAL SECURITY AUDIT PROCESS

The following CIP-014 compliance steps summary describes the major components generally considered essential to any utility physical security program. The protocol is intended to be a means by which an electric utility may identify those critical assets whose impairment would have significant impact, and for determining those investments that would have the greatest impact in reducing the risk of major and cascading outages.

***Initial Risk Assessment, R1***

A risk assessment is performed on applicable facilities which are typically a subset of the overall portfolio of utility transmission assets. A specific risk assessment approach is not specified in the standard. This risk assessment must consider factors such as loss of communications, cascading outages, and impact on the bulk electric system. Risk assessments must be performed for individual assets and may not be combined.

***Third Party Verification, R2***

A third party such as a security firm must verify the initial physical security risk assessment by reviewing and verifying documents and data from the transmission owner. If the third party arrives at a different finding, the transmission owner may modify its assessment or document any technical basis for not modifying.

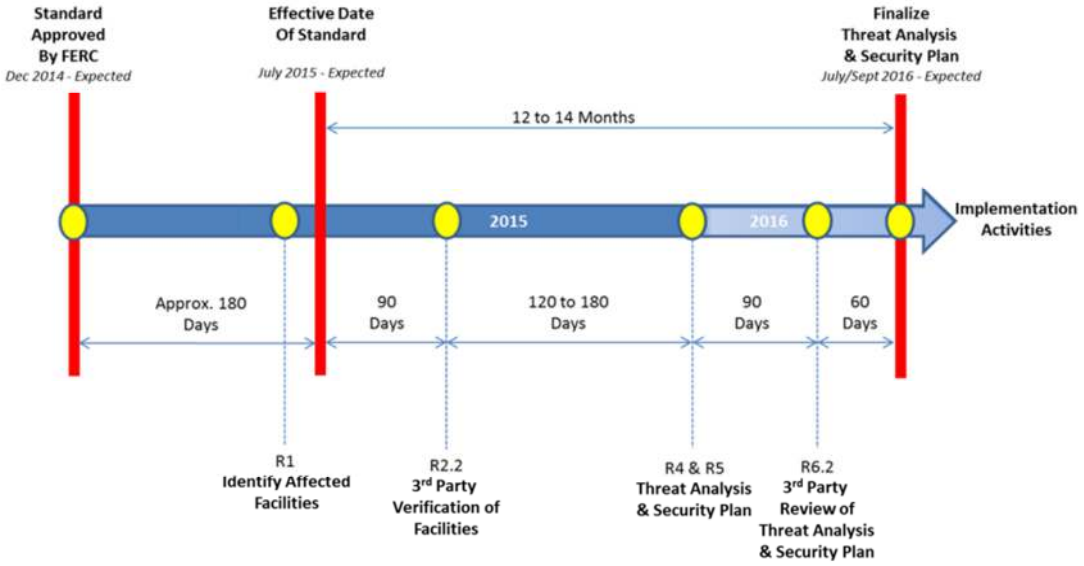
***Evaluation of Threats and Vulnerabilities, R4***

Any transmission owner that identifies a transmission asset subject to Requirement R1 and that is verified according to Requirement R2, shall conduct an evaluation of the potential threats and vulnerabilities of a physical attack for each of their respective assets. The evaluation must consider unique characteristics of the asset, prior history of attacks on similar facilities, and any intelligence or threat warnings received from sources such as local law enforcement, state or Federal agencies.

Next, a second review is to be conducted by a qualified third party to verify that the transmission owner conducted a robust threat and vulnerability assessment (TVA) of a physical

attack for each critical transmission asset identified in R1, and verified according to R2, and that the assessment included appropriate mitigation measures.

**Diagram 1. Expected timeframe for security plan implementation after CIP-014 protocol approved by FERC**




**Source:** FERC CIP-014 Protocol

***Physical Security Plan, R5***

Each transmission owner shall develop and implement a physical security plan for each critical transmission asset. The plan shall include:

- Resiliency or security (mitigation) measures intended collectively to deter, detect, delay, assess, communicate, and respond to potential physical threats and vulnerabilities identified during the evaluation conducted in Requirement R4;
- Up to date and accurate law enforcement contact and coordination information;
- A timeline for executing the physical security enhancements and modifications;
- Provisions to evaluate evolving physical threats and their corresponding security measures.

***ERO Audit of Security Plan, R6***

Each Transmission Owner must have each preliminary security plan[65] audited by the NERC-designated responsible entity region. As described above, in the western states region including California, such an audit would be performed by WECC.[66, 67]

[65] Review and verification of 1) the threat evaluation completed under Requirement R4 and 2) the unaffiliated third party review and the security plan(s) developed Requirement R5.

[66] WECC is the Western Electricity Coordinating Council and is the designated Electric Reliability Organization to the NERC for the western region. In this capacity WECC is a full-time regulatory authority that promotes CIP-014

# APPENDIX 2| FERC Information Sharing Definitions

**Critical Electric Infrastructure Information** is defined by the FERC as information related to critical electric infrastructure, or proposed critical electrical infrastructure, generated by or provided to the FERC or other Federal agency other than classified national security information, that is designated as critical electric infrastructure information by the FERC or the Secretary of the Department of Energy pursuant to section 215A(d) of the Federal Power Act.[68]

**Critical Energy Infrastructure Information (CEII)** is defined as specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure that:

> **(i)** Relates details about the production, generation, transportation, transmission, or distribution of energy;
>
> **(ii)** Could be useful to a person in planning an attack on critical infrastructure;
>
> **(iii)** Is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552; and
>
> **(iv)** Does not simply give the general location of the critical infrastructure.

**Critical electric infrastructure** is defined as a system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters.

standards and other electric security objectives by way of education and enforcement. More at http://www.nerc.com/pa/comp/Resources/ResourcesDL/2017_ERO_CMEP_IP.pdf

[67] Concurrent with the implementation of CIP-014, physical security audits by approved third parties were initiated in 2016. These audits include facility visits and inspections to determine if CIP-014 security plans are being appropriately implemented by transmission owners and to verify that proposed mitigations are appropriate solutions for the set of security concerns identified. Audit findings are confidential and privy to the WECC, the NERC/FERC, and the transmission owner. Regulatory Commissions such as the CPUC may not access these audit records.

[68] Critical Electric Infrastructure Information is exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C. 552(b)(3).

**Critical infrastructure** is defined as existing and proposed systems and assets, whether physical or virtual, the incapacity or destruction of which would negatively affect security, economic security, public health or safety, or any combination of those matters.

**Criteria and procedures for determining what constitutes CEII**

The following criteria and procedures apply to information labeled as CEII:

**(1)** For information submitted to the FERC:

**(i)** A person requesting that information submitted to the FERC be treated as CEII must include with its submission a justification for such treatment in accordance with the filing procedures posted on the FERC Web site at http://www.ferc.gov. The justification must provide how the information, or any portion of the information, qualifies as CEII, as the terms are defined in paragraphs (c)(1) and (2) of this section. The submission must also include a clear statement of the date the information was submitted to the FERC, how long the CEII designation should apply to the information and support for the period proposed. Failure to provide the justification or other required information could result in denial of the designation and release of the information to the public.

**(ii)** In addition to the justification required by paragraph (d)(1)(i) of this section, a person requesting that information submitted to the FERC be treated as CEII must clearly label the cover page and pages or portions of the information for which CEII treatment is claimed in bold, capital lettering, indicating that it contains CEII, as appropriate, and marked "DO NOT RELEASE." The submitter must also segregate those portions of the information that contain CEII (or information that reasonably could be expected to lead to the disclosure of the CEII) wherever feasible. The submitter must also submit to the FERC a public version with the information where CEII is redacted, to the extent practicable.

**(iii)** If a person files material as CEII in a complaint proceeding or other proceeding to which a right to intervention exists, that person must include a proposed form of protective agreement with the filing, or identify a protective agreement that has already been filed in the proceeding that applies to the filed material.

**(iv)** The information for which CEII treatment is claimed will be maintained in the FERC's files as non-public until such time as the FERC may determine that the information is not entitled to the treatment sought. By treating the information as CEII, the FERC is not making a determination on any claim of CEII status. The FERC retains the right to make determinations with regard to any claim of CEII status at any time, and the discretion to release information as necessary to carry out its jurisdictional responsibilities. Although unmarked information may be eligible for CEII treatment, the FERC will treat unmarked information as CEII only if it is properly designated as CEII pursuant to FERC regulations.

**(v)** The CEII Coordinator will evaluate whether the submitted information or portions of the information are covered by the definitions in paragraphs (c)(1) and (2) of this section prior to making a designation as CEII.

**(vi)** Subject to the exceptions set forth in paragraph (f)(5) of this section, when a CEII requester seeks information for which CEII status has been claimed, or when the FERC itself is considering release of such information, the CEII Coordinator or any other appropriate FERC official will notify the person who submitted the information and give the person an opportunity (at least five business days) in which to comment in writing on the request. A copy of this notice will be sent to the requester. Notice of a decision by the FERC, or the CEII Coordinator to make a release of CEII, will be given to any person claiming that the information is CEII no less than five business days before disclosure. The notice will respond to any objections to disclosure from the submitter that are not sustained. Where applicable, a copy of this notice will be sent to the CEII requester.

**Duration of the CEII designation**

All CEII designations will be subject to the following conditions:

**(1)** A designation may last for up to a five-year period, unless re-designated. In making a determination as to whether the designation should be extended, the CEII Coordinator will take into account information provided in response to paragraph (d)(1)(i) of this section, and any other information, as appropriate.

**(2)** A designation may be removed at any time, in whole or in part, if the FERC determines that the unauthorized disclosure of CEII could no longer be used to impair the security or reliability of the bulk-power system or distribution facilities or any other form of energy infrastructure.

**(3)** The FERC will treat CEII or documents marked as CEII as non-public after the designation has lapsed until the CEII Coordinator determines to un-designate the information.

**(4)** If a CEII designation is removed, the submitter will receive notice and an opportunity to comment. The CEII Coordinator will notify the submitter of the information and give the submitter an opportunity (at least five business days) in which to comment in writing prior to the removal of the designation. Notice of a removal decision will be given to any submitter claiming that the information is CEII no less than five business days before disclosure.

**CEII Coordinator**

FERC designates staff to serve as a CEII Coordinator. This role is responsibilities for reviewing all requests for CEII designations, determining whether the information meets CEII criteria.

FERC has established procedures through 18 CFR 388.112 for designating information contained in a particular document as privileged. Any party requesting that material be treated as privileged information must include a justification for such treatment and how information qualifies as CEII as defined in Federal Regulations. They must also provide how long the CEII designation should apply to aforementioned information. This information is evaluated by the CEII Coordinator to determine if the submitted information is covered by the FERC definitions in CEII.

# APPENDIX 3 | LOG OF PUBLIC WORKSHOPS

**Workshop 1, Cal-OES Headquarters, Mather, May 2, 2017**

*Topics:*

- Information Sharing for Critical Infrastructure Protection
- Establishing Proceeding Rules of Engagement for Input and Testimony on Sensitive Subjects
- Establishing Protocols for Data Access and Transfer

**Workshop 2, CPUC Headquarters, San Francisco, May 31, 2017**

*Topics:*

- Grid Security and Resiliency According to NERC
- CIP-014 Regulations and Implementation
- SMUD Case Study
- Distribution System Risk and Resiliency Best Practices

**Workshop 3, Southern California Edison Headquarters, Rosemead, June 21, 2017**

*Topics:*

- Physical Security Assessments
- Incident Response and Resiliency
- Tracking Physical Security Incidents
- Distribution System Risk Resiliency and Vulnerability Prevention
- Utilities Straw Proposals

**Workshop 4, CPUC Headquarters, San Francisco, September 29, 2017**

*Topics:*

- Joint Utilities Straw Proposal
- Qualifications of Third Party Reviewers
- CPUC White Paper

**Physical Security of Electric Facilities|R.15.06.009|CPUC Safety and Enforcement Division**
**May 2, 2017 | Workshop 1 | 9:30 a.m. to noon**
**CalOES Offices|3650 Schriever Avenue, Room MPR 1 & 2 | Mather, CA**

**W O R K S H O P  A G E N D A**

**9:30- 10:00 a.m. Opening Remarks by CPUC President *Michael Picker*, Commissioner *Cliff Rechtschaffen,* and Administrative Law Judge *Gerald Kelly***

**10:00 – 10:15 am Opening Remarks by Director of the Governor's Office of Emergency Services, *Mark Ghilarducci (delayed)***

**10:15 - 10:30 a.m. Overview of the Proceeding, *Laying the Ground Rules for Getting It Right, Arthur O'Donnell, SED Risk and Safety Supervisor, CPUC***

**10:40- 11:40 a.m. Two-part Panel Discussion**

**Who Needs to Know – Balancing Security with Collaboration: *Information Sharing for Critical Infrastructure Protection***

- Determining the extent to which closed door sessions are desirable and warranted
- Determining who gets access and who does not
- Recommendations on qualifying criteria for individuals and entities
- Recommendations on any appropriate new protocols

**Overview of Information Categories**

- Existing information categories
- Any proposed new information categories and whether existing practices are sufficient

**Moderated by *Arthur O'Donnell, SED Risk and Safety Supervisor***

**Panelists**

- ***Scott Aaronson, Executive Director, Security and Business Continuity, Edison Electric Institute***
- ***Herb Brown, Director, Sacramento Fusion Center,***
- ***John Pespisa, Director of Compliance, SCE***
- ***Christopher Vicino, Director of Security and Emergency Management, LADWP***

**11:40 - noon When to Invoke PU Code Sec. 364(d) To Protect Critical Infrastructure**

**Brainstorming and Consensus Exercise Facilitated by SED staff**

**Noon ADJOURN**

**Physical Security of Electric Facilities|R.15.06.009|CPUC Safety and Enforcement Division**
**May 31, 2017 | Workshop 2 | 9:30 a.m. to 4:00 p.m.**
**CPUC Auditorium |505 Van Ness Avenue| San Francisco, CA**

**W O R K S H O P  A G E N D A**

**9:30- 9:35 a.m.** **Welcome and Introductions**

***Topic Area #1: Federal Statutes and Guidelines to Address Physical Security***

***Part 1: NERC National Perspective***

**9:35- 10:45 a.m.** **Grid Security and Resiliency According to the NERC**

Carl Herron – North American Electric Reliability Corporation (NERC)

**10:45- 10:55 a.m.** **B R E A K TEN MINUTES**

**10:55- noon** **CIP-014 | Critical Infrastructure Protection | Federal Rules Overview, Applicability, and Update on Implementation Rollout**

Darren Nielsen – Manager, Cyber & Physical Security Audits, Western Electricity Coordinating Council

Richard Hyatt – Chair WECC Physical Security Work Group, Chelan County (Washington) PUD

John Pespsia – Director of NERC Compliance, SoCal Edison

**Noon- 1:15 p.m.** **L U N C H – one hour, 15 minutes**

***Part 2: California Lens Perspective***

**1:15- 2:00 p.m.** **SMUD's Tenfold Drop in Facility Intrusions in Two Years – "*Protect Your Borders*" Paper Presentation**

James Day, paper author, Sacramento Municipal Utility District

**2:00- 2:40 p.m.** **Distribution System Risk and Resiliency Best Practices Discussion**

**Crowdsourced brainstorming and input exercise facilitated by SED staff**

**2:40- 2:55 p.m.** **B R E A K FIFTEEN MINUTES**

**2:55- 3:40 p.m.** **Achieving CIP-014 and PU Code Seamlessness: Weeding Out Potential Gaps and Areas of Redundancy and Conflict**

**Crowdsourced brainstorming and input exercise facilitated by SED staff**

**3:40– 4:00 p.m.** **Summary Recap and Roundup, SED staff**

**4:00 p.m.** **A D J O U R N**

**Physical Security of Electric Facilities|R.15-06-009|CPUC Safety and Enforcement Division**
**June 21, 2017 | Workshop 3 |9:30 a.m. to 3:30 p.m.**
**SoCal Edison | 2244 Walnut Grove Ave.| Rosemead, CA**
**W O R K S H O P  A G E N D A**

**9:30- 9:35 a.m.** **Welcome and Introductions**

**9:35- 10:05 a.m.** **What Are We Protecting Against? California Theft Intrusions Threat: Insurance Industry Stats and U.S. DOE OE-417 Electric Disturbance Event and Incident Reports**

SED staff presentation by Martin Kurtovich

**10:05- 10:45 a.m.** **Physical Security Assessments: Threat Vulnerability and Security and Mitigation Plans, *a Consultant Expert Perspective on CIP-014 Compliance***

Harford Field III, Corporate Risk Solutions, Inc., Manager Consulting Services

**10:45- 10:55 a.m.** **B R E A K TEN MINUTES**

**10:55- 11:45 a.m.** **Incident Response and Resiliency Presentation, Part I**

*Emergency preparedness and response plans, IOU perspective*
Thomas Jacobus, SCE, Principal Manager, Business Resiliency
Robert Kang, Senior Attorney, SCE

**11:45- 1:15 p.m.** **L U N C H – one hour, 30 minutes**

**1:15- 1:45 p.m.** **Incident Response and Resiliency Presentation, Part II**

*Emergency preparedness and response plans, POU perspective*

Stephen E. Lafond, Riverside Public Utilities, Principal Engineer in Substation, Transmission, and Distribution Standards (Energy Delivery)

**1:45- 2:25 p.m.** **Distribution System Risk Resiliency and Vulnerability Prevention Panel Discussion**

*Spare parts inventories, dispatch, and change-outs; deployment of mobile generator units; distribution system design, redundancy, and resiliency; backup capabilities such as switching, back-ties, and load transfer; equipment and best practices sharing strategies.*

Raymond Trinh, PG&E, Manager in Substation Asset Strategy and Reliability
Stephen E. Lafond, Riverside Public Utilities, Principal Engineer
Alex Salinas, SCE, Principal Manager, Technical Support
Moderated by Arthur O'Donnell, SED Risk and Safety Assessment Supervisor

**2:25- 2:30 p.m.** **B R E A K FIVE MINUTES**

**2:30- 3:30 p.m.** **Utility Straw Proposal**
Presentations by the utilities and discussion

**3:30 p.m.** **A D J O U R N**

**Physical Security of Electric Facilities|R.15-06-009|CPUC Safety and Enforcement Division**
**September 29, 2017 | Workshop 4 |10:00 a.m. to 3:30 p.m.**
**CPUC Courtyard Room | 505 Van Ness Avenue| San Francisco**

**W O R K S H O P  A G E N D A**

**10:00- 10:15 a.m.** **Welcome and Introductions**

**10:15- Noon** **Joint-Utility Straw Proposal for New California Standards for Electric Distribution Asset Physical Security Plan Review, Adoption, and Maintenance**

Presentations by the utilities, followed by Q&A

Spotlight on select issues:

1. Security plan review and approval
2. Balancing accounts v. GRCs
3. Sensitive information – D. 16-08-024 confidentiality rules
    - specifying categories of potential "unaffiliated third parties"
    - defining "security-sensitive" information
4. Essential customers, and consideration of trauma centers and nursing homes
5. Commission jurisdiction and POUs

**Noon- 1:15 p.m.** **L U N C H – one hour, 15 minutes**

**1:15- 2:00 p.m.** **Physical Security Plan Consultant Services | Minimum Qualifications for Establishing Third-party Reviewer Competency**

Group discussion with SED and utility staff

**2:00 p.m.** ***Break*** **– 10 minutes**

**2:10- 2:50 p.m.** **Physical Security Proceeding Scoping Memo Recap and SB 699 Directives Recap and Retrospective**

*A consensus-seeking exercise led by SED staff to recount those items originally believed to have been valid, applicable, and timely and to determine if circumstances have changed such that certain items are now considered as non-essential, and to tally any items not addressed thus far*

**2:50- 3:30 p.m.** **SED Staff White Paper on Physical Security Plan Update and Overview**

Presentation by SED staff, followed by Q&A

**3:30 p.m.** **A D J O U R N**

## APPENDIX 4 | SB 699 AS CHAPTERED:

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.

BILL TEXT

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:

(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.

###