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.

Because of the experience that 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.

Excerpted from January 2018 Physical Security Staff White Paper

- 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.