BEFORE THE PUBLIC UTILITIES COMMISSION

OF THE STATE OF CALIFORNIA

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

Safety & Enforcement Division's Risk Assessment & Safety Advisory (RASA) section evaluation of the Joint Utility Proposal and Recommendations for Consideration

Arthur O'Donnell, Program and Project Supervisor

Marty Kurtovich, PE, Senior Utilities Engineer

Jeremy Battis, Senior Regulatory Analyst

January 4, 2018

Note: SED Risk Assessment and Safety Advisory section (RASA) is not a Party in this proceeding, but provides advisory support to the Administrative Law Judge and Assigned Commissioner. RASA organized four workshops for the rulemaking and conferred with Parties in the drafting of the Joint Utility Proposal and public discussions of its provisions. Separately, SED's Electric Safety & Reliability Branch (ESRB) is an Active Party and has provided written comments on the Joint Utility Proposal.

Procedural Background

On August 31, 2017, ten parties participating in the Rulemaking 15-06-009 proceeding filed a document entitled the Joint Parties' Filing of Updated Draft Straw Proposal for Physical Security Regulations (Straw Proposal).[1]

This proceeding was initiated by Senate Bill 699[2] which required the Commission to develop rules for addressing physical security risk to the distribution systems of electrical corporations. Section 364 further states (in part),

> *"The standards or rules, which shall be prescriptive or performance based, or both, and may be based on risk management, as appropriate, for each substantial type of distribution equipment or facility shall provide for high-quality, safe and reliable service."* And,
>
> *"In setting its standards or rules, the commission shall consider: cost, local geography and weather, applicable codes, potential physical security risks, national electric industry practices, sound engineering judgement, and experience."*

In order to meet the requirements of SB 699, the Safety and Enforcement Division initiated a series of physical security workshops from May to September 2017.

Existing public utility law does not otherwise specifically address physical security risks associated with distribution assets. The only regulations addressing the physical security of electric utility assets are those developed for Critical Infrastructure Protocols (CIPs) developed at the national level under the auspices of the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC).

The first three workshops were intended to identify and explore the current regulatory framework under which California electric utilities address physical security for its assets, existing utility physical security activities, and how new regulations should be crafted and support the risks associated with the physical security of electric distribution systems as specified in SB 699.

[1] Hereafter, the Straw Proposal will be referred to as the Joint Utility Proposal or the Proposal.

[2] SB 699 (Hill-2015) amending Public Utilities Code Section 364

In conjunction with these workshops, a technical work group was formed by ten parties in the proceeding.[3] These entities developed a Joint Proposal to provide a mechanism for compliance with Sec. 364 that would apply to both the CPUC jurisdictional utilities as well as to publicly-owned entities.

A. Summary of the Joint Proposal

The Proposal describes how a utility should establish a Distribution Substation and Distribution Control Center Security Program (Distribution Security Program). This program consists of 1) Identification of distribution facilities, 2) assessment of physical security risk on distribution facilities, 3) development and implementation of security plan, 4) verification, 5) record keeping, 6) timelines and, 7) cost recovery.

The utilities' Proposal would introduce new requirements that address electric assets that support distribution-level service, within California regulatory and safety jurisdiction. These assets, largely substations and control centers, do not rise to the level of "critical infrastructure" as defined under the federal CIPs program, which relates to high-voltage transmission and substation facilities. However, they are essential for providing reliable energy to residential, commercial and industrial loads.

The proposed mechanism for the risk assessment of such assets, the prioritization of security protections against physical attack or intrusion, and the implementation of potential mitigations to ensure system resiliency in the event of such an incident, represent a first-of-its kind effort at the state level.

The Proposal would introduce two new primary physical security elements to existing Commission requirements addressing distribution assets:

1) A process for standardized implementation of a Distribution Substation and Distribution Control Center Security Program (Distribution Security Program) and development of Mitigation Plans covering facilities that meet certain criteria, and,

[3] Bear Valley Electric Service, California Municipal Utilities Association, Los Angeles Department of Water & Power. Liberty CalPEco, National Rural Electric Cooperative Association, PacifiCorp, Pacific Gas & Electric Company. Sacramento Municipal Utility District, San Diego Gas & Electric Company, and Southern California Edison Company.

2) Procedures for Exchange of and Access to Highly Confidential and Sensitive Information.

The eventual Mitigation Plans envisioned by this process could include a mix of strategies: hardening of physical assets (i.e., walls, gates), increased security monitoring measures (eg., video surveillance, gunshot detectors, patrols, etc), or actions and programs to increase the resilience of the distribution network in the event of an adverse incident. It would be up to each utility to identify a cost-effective and optimal protection plan.

The Joint Proposal reflects initiative and a cooperative spirit among its proponents, both investor-owned utilities (IOUs) subject to the Commission's full regulatory authority, and among publicly-owned utilities, agencies, departments, boards and co-ops (collectively, POUs), which each have their own governance structures, but are subject to CPUC jurisdiction for the provision of safe and reliable electric services.

SED RASA is encouraged by this cooperative effort, and finds the Joint Proposal to be a workable approach to assuring California energy users that the utilities and the Commission are serious about safeguarding these important assets. While generally supportive of the Joint Proposal, SED RASA recommends some additional provisions and considerations, along with the flexibility that would accommodate inherent differences between IOUs and POUs.

SED RASA proposes a somewhat more detailed approach to the creation of the Security Program and Mitigation Plans (The Six-Step Process described below), to bring the process closer in line with the CIPs program overseen by NERC

Other proposed modifications to the Joint Proposal are meant to:

- Clarify Commission oversight authority and access to documentation;
- Protect against unauthorized access to Confidential or Security-Sensitive Information;
- Augment the criteria that utilities propose to use for determining "priority assets" subject to the Security Program by adding consideration of assets that provide electric service to "essential customers" and vulnerable populations.

- Better define the criteria for third-party verification of the Distribution Security Programs and Mitigation Plans, and;
- Expedite the time table for utilities to provide an assessment of their assets and the approval of plans for compliance with this new program.
- Supplement reporting requirements to fill in gaps in the CPUC's incident reporting policy.

With these modifications, SED RASA believes that Commission and the utilities will be able to agree to a model approach to physical security in the state, and provide national leadership that can inform the actions of other state regulatory agencies and utilities across the nation.

B. Principles of the Joint Utility Proposal

In accord with the general direction of SB 699, the Utility Proposal asserts an intention to develop "a risk management approach towards distribution system physical security, with appropriate consideration for resiliency, impact and cost."[4]

The Proposal states a set of general principles that derive from information described and discussed in the series of workshops that SED RASA organized as part of the rulemaking:

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

[4] Straw Proposal, part 1 (3), page 1.

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

SED RASA endorses the principles, and would add the following considerations which also arise from the discussions among parties in workshops and the Technical Working Group, and in Staff's findings embodied in the recently released "white paper":[5]

- Costs of incremental physical security measures should be reasonable, controlled, and weighed against potential benefit, so they do not result in a burden to ratepayers.
- Opportunities to incorporate high-benefit, low-cost measures should be captured, particularly at the time of new or upgraded substation construction.
- Distribution assets to be hardened, or to be designated as a priority for service restoration and reliability, should be designated with consideration for ensuring service integrity to essential customers, among the other factors identified in the Joint Proposal.
- Resiliency strategies to ensure that priority distribution assets -- particularly those tied to service to essential customers -- remain in service and are able to rapidly recover from an unplanned service outage should be considered an equally effective response to addressing physical security risks.

C. Proposed new requirements in Joint Proposal

[5] SED report, "Security and Resilience for California Electric Distribution Infrastructure: Regulatory and Industry Response to SB 699", January 2018.

The Proposal would introduce two new primary physical security elements to existing Commission requirements addressing distribution assets: 1) A process for standardized implementation of a Distribution Substation and Distribution Control Center Security Program (Distribution Security Program) and development of Mitigation Plans covering facilities that meet certain criteria, and 2) Procedures for Exchange of and Access to Highly Confidential and Sensitive Information.

The elements of the Security Program can be boiled down to:

- Each Distribution System Operator will establish a Distribution Substation and Distribution Control Center Security Program (Distribution Security Program);
- Each Operator will identify which, if any, of its Distribution Facilities meet the criteria set forth in the Proposal
- Operators will evaluate the potential risks associated with a physical attack on each of the identified Distribution Facilities meeting the criteria and assess whether existing grid resiliency and/or physical security measures appropriately mitigate the risks.
- Those identified Distribution Facilities that do not have existing grid resiliency and/or physical security measures necessary to appropriately mitigate the risks will be considered "Covered Distribution Facilities."
- For each of its Covered Distribution Facilities, an Operator will then develop a Mitigation Plan to document the strategy for mitigating the risk and/or consequences of an attack on the Covered Distribution Facility.
- An unaffiliated third-party will review (1) the process used by Operators to identify the Covered Distribution Facilities and (2) the Mitigation Plan(s) developed by Operators to reduce the risks and/or the consequences of an attack on Covered Distribution Facilities.
- Each Operator will review each of its Mitigation Plans at least once every five years.

The straw proposal then defines a process for the utility to evaluate the potential risk associated with a successful physical attack on distribution facilities that meet the above criteria. This evaluation includes:

1) A determination of existing grid resiliency;

2) Requirements for customer-owned back-up generation;

3) Existing physical security measures appropriately mitigating these risks;

4) Availability of spare assets to restore power;

5) Potential for emergency responders to identify and respond to an attack;

6) Location and physical surroundings, history of criminal activity at facility and in the area;

7) Availability of back-up generation or energy storage at customer sites; and,

8) Availability of alternative means to serve impacted load such as a back-up command center.

In detailing how a utility will develop and implement a mitigation plan to address the potential risk of a long-term outage to a covered distribution facility due to a physical attack the straw proposal states that utilities may use risk-based performance standards to identify the upgrade a facility's security. It elaborates that a performance standard specifies the outcome required but leaves the specific measures to achieve this outcome up to the discretion of the utility.

For distribution facilities whose risk are not adequately mitigated by existing measures or grid resiliency, the Proposal defines these as "covered" distribution facilities subject to development of a physical security mitigation plan.

The Joint Proposal does not provide any detail on or examples of such performance standards nor does it define a process for making risk-based decisions. It does provide examples of potential resiliency solutions such as strategically located spares or adding circuit ties to add additional operation flexibility and security solutions such as improved access control measures and collaboration with local law enforcement.

The Joint Proposal then addresses verification of the mitigation plan via an unaffiliated third party with appropriate experience. Based on this review, the utility will either modify its plan or document reasons for not doing so.

The Joint Proposal then stipulates what records of the utility's Distribution Security Program will maintain as electronic or hard copies for not less than five (5) years. The proposal states that maintained records are "extremely" confidential and will be maintained in a secure manner at the utility's headquarters and will be available for inspection.

According to the Joint Proposal, a utility will complete an initial draft of its mitigation plans within eighteen (18) months from the effective date of the guidelines. The utility is allowed 27 months to obtain third-party verification of the mitigation plans. Each utility is directed to meet its obligations within thirty (30) months of the effective date of the guidelines/Joint Proposal.

Lastly, this section of the Joint Proposal addresses cost recovery, stating that the utility may establish an account to track the expenditure associated with the development and execution of its Distribution Security Program. It allows for cost recovery for investor-owned utilities to be through a separate application or GRC request.

It instructs utilities to file a public version of the unaffiliated third-party review and Commission approval in support of their cost recovery requests.

Discussion

To a large degree, this process mimics and draws upon those that have been developed under the federal Critical Infrastructure Protocols for physical security of critical electric assets (CIP-014).[6] CIP security plans under NERC-FERC requirements as they have now become mandatory after an extended "voluntary compliance" grace period. It should be emphasized that CIP-14 concerns itself with the potential for a concerted, terrorist attack on utility infrastructure that could result in severe damage, cascading outages on the grid, and longer-term disruption to utility service across a regional electric grid.

CIP security plans generally provide multiple levels of site and facility analysis, coupled with risk, threat, and vulnerability assessments. A signature feature of the CIP security plan process is its reliance on multiple *validation* steps wherein a

[6] In several instances, this Staff evaluation will refer to the federal Critical Infrastructure Protocol for electric transmission facilities (CIP-014) and make comparisons or contrasts with the Utility Proposal and the Staff recommended modifications. Table A is attached to this document that may provide a helpful guide to these difference and similarities.

third-party with varying levels of impartiality critiques and signs off on findings and proposed mitigation measures. The final stage in the CIP security plan validation process is the *plan audit* wherein a utility submits a proposed final *plan report* to its NERC-designated regulatory enforcement entity[7] to accept as adequate and complete. A CIP security plan report would consist of various component assessments, consultant opinions and recommendations, a mitigation plan detailing consultant-recommended measures, and a utility statement to accept or decline recommended mitigation measures.

The utilities' Proposal would introduce new requirements that, although not as rigorous as NERC CIP guidelines, are intended to address electric assets considered well less critical and important than those under NERC-FERC oversight.

Two major differences between NERC CIP and the utilities' Proposal are that: 1) NERC CIP requires a targeted security plan for each individually identified critical asset; the utilities' methodology by contrast, would each complete one blanket security plan for all "priority" distribution assets; and 2) the utilities' propose to consolidate or eliminate several of the five steps in the security plan process prescribed by NERC CIP.

D. SED Staff Appraisal of Joint Utilities Proposal, Security Plan Element

The Joint Proposal would commit all California electric utilities to identifying those distribution *priority assets*[8] that merit any special protection and measures, would develop mitigation plans to lessen identified risks and threats, and would incorporate the expertise of an independent third-party reviewer.

Stakeholder input and SED RASA review have identified areas where the proposed security plan requirements would be improved by providing more

[7] For California and other western states this designated regional "Electric Reliability Organization" is "WECC," or the Western Electricity Coordinating Council.

[8] The Utility proposal does not use the term "priority assets" but rather "Covered Distribution Facility" which are distinguished from "critical assets" under the Federal CIP program. This is one of a number of instances where slight modification to the language employed by utilities might be helpful. Attached to this document, SED RASA has provided a table of terms that appear to be comparable in meaning but distinct in their usage. The Commission may wish to consider taking comments on adjustments to terminology for consistency sake.

granularity and specificity surrounding new requirements for distribution system security plans.

As one example, the Proposal fails to mention or describe the Commission's role in the review and approval of security plans; the compliance process including CPUC-issued sanctions or penalties for non-compliance: and maintenance requirements for ensuring the continued effectiveness of security plans.

The Proposal would be strengthened by more specific description of the role and timing of third-party reviewers and the criteria and process for how a utility might decline a recommended mitigation measure.

The Proposal's description for those distribution facilities to be subject to security plan requirements could be more detailed, with improved linkages to customers deemed essential.[9]

A Six-step Security Plan Process Advanced by SED

SED recommends the following six-step procedure for carrying out new physical security plan ("security plan" or "plan") requirements to address utilities' distribution assets. The proposed six steps are modeled on security plan requirements prescribed by NERC CIP-014.

[9] Public Utilities Code Section 2771, adopted in 1976, directs the Commission to establish priorities among categories of customers. GO 166 defines essential customers as those requiring electric service to ensure availability of public health and safety services. D.01-05-089 specifies these categories as:

- Government and other agencies providing essential fire, police, and prison services
- Government agencies essential to the national defense
- Hospitals
- Communication utilities, as they relate to public health, welfare and security, including telephones
- Navigation communication, traffic control, and landing and departure facilities for commercial air and sea operations
- Electricity utility facilities and supporting fuel and fuel-transportation services critical to continuity of electric-power system operation.
- Radio and television broadcasting stations used for broadcasting emergency messages, instructions and other public information related to electricity-curtailment emergencies
- Water and wastewater treatment utilities during emergencies that require their services, such as fire fighting
- Rail transit systems as necessary to protect public safety

SED staff recommends including vulnerable elderly populations, which may be housed in convalescent or hospice facilities.

- Step 1. Assessment. Drafting of a plan, addressing prevention, response, and recovery, which could be prepared in-house[10] or by a consultant.
- Step 2. Independent Review and Utility Response to Recommendations. Proposed plan would be "reviewed" and deemed appropriate and adequate by some independent third party, likely a qualified consultant expert, national laboratory, or a regulatory or industry standard body (such as the Electric Power Research Institute. Step 2 would include reviewer recommendations, including mitigation measures. Utilities would be expected to fully address reviewer recommendations, including justifying any mitigations that it declines to accept; the independent third-party opinion/recommendations, utility response, threat and risk assessment, and mitigation measures combined would constitute a final plan report.
- Step 3. Validation (for IOUs only). Final plan report would be validated (recurring every five years)[11] so as to deem it adequate, in compliance, and eligible to request funding for implementation.[12] The validation would be performed by the CPUC Safety and Enforcement Division (SED). Non-compliance may be met with a violation order to be followed up with sanctions and/or penalties by SED.
- Step 3a. Validation (for POUs only). Final plan report would be validated by a qualified authority designated by the applicable local governance body. (For example, Riverside Public Utilities currently develops a security and emergency response plan that conforms to CalOES and FEMA standards and receives their endorsement.)
- Step 4, Adoption. Validated plan would be submitted to the appropriate regulatory oversight body (for IOUs, the CPUC; for POUs, their local governance body) for review and greenlighting (adoption). Step 4 should include funding to implement the plan.
- Step 4a. (for POUs only). Notice. Provide CPUC with official notice (ideally including a copy of a resolution) of the adopted plan action.

[10] In-house work would require utility staff who have CIP-014 qualifications

[11] This time interval is based on the requirements instituted for the City of Los Angeles under City Charter.

[12] Upon five years from the date of adoption, a utility would be required to have any revised or original plan updated and repeat the validation process. Utilities may be afforded regulatory relief by way of an exemption request process for special cases where undertaking of the plan overhaul and/or validation processes may be impracticable or unduly burdensome.

- Step 5. Maintenance. Ongoing adopted plan refinement and updates as appropriate and as necessary to preserve plan integrity. All security plans should be concurrent with and integrated into utility resiliency plans and activities.
- Step 6. Repeat Process. Plan overhaul and new validation after five years.

Additional Recommendations for Mitigation Plans

Additionally, SED RASA would recommend these requirements and clarifications:

- The Commission should consider requiring California electric utilities, within any new or renovated distribution substation, to incorporate and design their facilities to incorporate reasonable security features.
- Utilities' security plans should include:
  - Specifics on efforts to support a supply-chain vulnerabilities goal (i.e., ensure the rapid dispatch of available spare parts and qualified service technicians);
  - A training program for appropriate local law enforcement and utility security staff to optimize communication during a physical security event. Training for law enforcement should include information on physical infrastructure and relevant utility operations;
  - A preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately;
  - A description of Distribution Control Center and Security Control Center roles and actions related to distribution system physical security (this final item would be for IOUs only); and
  - A determination of the vulnerability of any associated communication utility infrastructure that supports priority distribution assets, which if deemed to be vulnerable, should have appropriate mitigation measures prescribed
- Utility distribution control center security programs should focus on development, implementation, refinement, and maintenance of:
  - security plans;

- a reliable reporting system for physical security incidents at distribution facilities; and
- information sharing protocols

E. Third-Party Verification

As with CIP-014, utilities would employ qualified experts to assess a facility and its risks and threats.[13] Unlike CIP-014, a third-party review of this phase and the resulting assessment work product would be *optional*. A required third-party review would occur later, in tandem with completion of a list of recommended mitigation measures.[14] The third-party reviewer would prepare a recommendation on appropriate mitigation measures and/or a statement supporting or not supporting proposed mitigation measures.

Utilities would then produce a response to proposed mitigation measures and the third-party expert's opinion and recommendation, indicating whether a utility concurs or disagrees, and whether a given mitigation measure is recognized and to be implemented, or is declined. Utilities should provide a justification for declining any proposed mitigation measures.

The risk-threat assessment, mitigation plan, consultant appraisal and statement, and utility response, would together comprise a *Security Plan*. The Security Plan should include some reasonable attempt at an estimated timeframe for completion and a cost estimate.

Discussion

SED RASA endorses the reliance on qualified third-party verification of the Distribution Security Program and Mitigation Plans. However, the Joint Proposal does not fully explain what qualifications are desirable in such independent experts. This issue was addressed in the September 29 workshop, with discussion of an IOU recommended set of criteria and definitions for eligibility.

- Unaffiliated Third Party Reviewer: An entity other than the Operator with appropriate expertise. The selected third party reviewer cannot be a

[13] Under CIP-014, generally referred to as risk assessment and threat assessment components
[14] This work product may collectively be called the Mitigation Plan

corporate affiliate (i.e., the third party reviewer cannot be an entity that corporately controls, is controlled by or is under common control with, the Operator). A third party reviewer also cannot be a division of the Operator that operates as a functional unit. A governmental entity can select as the third party reviewer another governmental entity within the same political subdivision, so long as the entity has the appropriate expertise, and is not a division of the Operator that operates as a functional unit, i.e., a municipality could use their police department if it has the appropriate expertise.

- Unaffiliated Third Party Reviewer Appropriate Expertise: An entity or organization with electric industry physical security experience and whose review staff has appropriate physical security expertise, i.e., have at least one member who holds either an ASIS Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; an entity or organization with demonstrated law enforcement, government, or military physical security expertise; or an entity or organization approved to do physical security assessments by the CPUC, Electric Reliability Organization or similar electrical industry regulatory body.

A more simplified description was provided by POU representatives:

- An entity or organization with electric industry physical security experience and whose review staff has at least one member who holds either a Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification;
- A governmental agency with physical security expertise; or
- An entity or organization with demonstrated law enforcement, government, or military physical security expertise.

Discussions during the workshops provide convincing evidence that such professionals are available to California utilities, and that the program outlined in the Utility Proposal provides sufficient flexibility in how utilities employ such expertise – whether to support the entire process of Identification, Assessment, developing Mitigation Plans, Verification and Records keeping, or simply providing verification of the resulting plans. The key is to have non-employee expertise available.

Recommendation

A third party reviewer may not be a corporate affiliate (i.e., the third party reviewer cannot be an entity that corporately controls, is controlled by, or is under common control with the utility). A third party reviewer also cannot be a division of the utility that operates as a functional unit. Such unaffiliated third party reviewer should be an entity or organization with electric industry physical security experience and whose review staff demonstrates appropriate physical security expertise, i.e., has at least one member who holds either an ASIS Certified Protection Professional (CPP) or Physical Security Professional (PSP) certification; an entity or organization with demonstrated law enforcement, government, or military physical security expertise; or an entity or organization approved to do physical security assessments by the CPUC, Electric Reliability Organization, or similar electrical industry regulatory body.

F. Access to Information

In the Proposal, the utilities have outlined an approach to sharing information about their Security Program development and Mitigations Plans with CPUC staff that does not entail the CPUC having possession of the documents.

- **Reading Room Approach:** A method for sharing Security-Sensitive Information with the Commission. Security-Sensitive Information will be available for inspection at the Operator's headquarters, or a mutually agreed-to location, by Commission staff upon request.
- **Security-Sensitive Information:** Information that if disclosed could negatively impact public safety or the safe and reliable operation of an Operator's system. Such information may only be shared with Commission staff using enhanced access controls, such as the Reading Room approach. Such information is exempt from the California Public Records Act.

Public access to *public information* would be afforded in accordance with the California Public Records Act. *Confidential Information* is defined in the Joint Proposal as information that the Commission determines exempt from the California Public Records Act. *Security-Sensitive Information* is information exempt from the California Public Records Act and which may be shared with

Commission staff only using enhanced secure access control measures, such as the *Reading Room approach*.

The proposed Reading Room approach would make security-sensitive information available in hard copy and available for Commission review at a utility's facilities. In some cases, the information may be made available for inspection by the Commission at the utility's San Francisco offices upon request.

Precedent for this approach can be found in NERC-FERC policies on information sharing related to CIP-014 and physical security of the bulk power system. The protocol stipulates that utilities will share physical security information with regulators, law enforcement, and first responders by making relevant information available in a secure setting on the utility's property.

The joint utilities have advanced a proposed solution that places a very high value on safeguarding of information, with less importance paid to convenience, accessibility, and functionality. The precedent for this so-called "reading room" approach is NERC-FERC guidance on information sharing tied to CIP rules. The protocol stipulates that utilities will share physical security information with regulators and appropriate law enforcement and first responders only by furnishing requested physical security hardcopy format at a utility's offices, which would ostensibly require an advance appointment, some waiting time and logistical coordination, and (for CPUC staff) foreseeable air travel.

While the reading room approach may be the default existing interim means for information sharing in the absence of clear adopted guidelines, SED staff has concerns about the practicality of the logistics.

It should be noted that the Commission is engaged in an effort to update its policies regarding the protection of Confidential Information in a rulemaking related to Public Records Act requests.[15] A recent decision has approved an update to General Order 66-D, which will take effect in January 2018. Parties to the proceeding have been tasked with developing matricies of the kinds of documents that fall under exemptions to PRA, per the State Government Code section.

[15] R.14-11-001, Order Instituting Rulemaking to Improve Public Access to Public Records Pursuant to the California Public Records Act.

Utilities have, in the past, cited reliance on Government Code § 6254(e), in seeking confidentiality of information about critical infrastructure. However, the Code section does not explicitly mention or imply "critical infrastructure":

> 6254. Except as provided in Sections 6254.7 and 6254.13, this chapter does not require the disclosure of any of the following records:
>
> (e) Geological and geophysical data, plant production data, and similar information relating to utility systems development, or market or crop reports, that are obtained in confidence from any person.

Additionally, there has been reliance on § 6254 (k) which is a broad category of "records, the disclosure of which is exempted or prohibited pursuant to federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege." The specific federal law would be 18 CFR 388.113, from FERC Order 883 December 21, 2006:

> 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.

SED RASA is mindful of the utilities' valid concerns that unauthorized release of critical asset data or documents could have a very harmful impact on reliable operations. There is a need for clarity about the nature of documents which rightly should be shielded from unauthorized public disclosure, whether considered "critical infrastructure" or the level of "priority assets" and mitigation plans envisioned in this proceeding.

However, it is without question that the Commission and its staff require and are fully entitled to access such information, as long as protections against public release are maintained. Especially in cases where the Commission is investigating an incident – whether it is already defined in our regulations or a new aspect, such as physical or cyber attack, access to records shall be proved at the Commission's demand, not at the convenience of the utilities.

The reading room approach, as proposed, is a workable interim solution and should for the time being, serve as the default information-sharing method.

Until such time that the Commission finalizes its rules for the safekeeping, sharing, transmittal, and inspection of confidential information, all findings of this review shall be made available on utility property agreed to by the Safety and Enforcement Division, or its successor.

G. Publicly Owned Utilities

The Joint Proposal also includes a statement from the California Municipal Utilities Association, Los Angeles Department of Water & Power, the National Rural Electric Cooperative Association and Sacramento Municipal Utility District that legislative mandates in SB 699 do not apply to publicly owned utilities, that the scope of this rulemaking do not include POUs and they are not subject to Commission enforcement jurisdiction.

POUs stated they are participating in the proceeding as a means to develop reasonable industry guidelines based on best practices. They contend that participation by the POUs does not concede or waive jurisdiction through their participation in this proceeding.

Discussion

RASA staff is gratified by the participation of the POUs in this rulemaking, and is encourage by the willingness to cooperate in developing the Joint Proposal and offer insights and expertise to the discussions.

Staff recommends that issues related the Commission's jurisdiction over health and safety matters, including physical security of infrastructure are best resolved via legal briefings in this proceeding.

What staff has learned through its research and presentations in workshops is that the larger POUs are already actively engaged in the federal CIPs process, and are in a good position to apply the Joint Proposal to priority assets at the distribution level. An excellent example was provided by the City of Riverside's Public Utilities Department.

Riverside Utilities described its emergency planning program, which includes analysis of projects to upgrade substations facilities. Riverside incident response and resiliency approach is informed and prompted by the Federal Disaster

Mitigation Act of 2000. The Riverside utility develops a Hazard Mitigation Plan to meet federal requirements.

The plan also enables the utility to apply for federal disaster preparation assistance. The plan is then reviewed and approved by 1) its local governance (the utility board and city council); 2) Riverside County; 3) California Office of Emergency Services; and 4) the Federal Emergency Management Administration (FEMA). Riverside's Critical Infrastructure Protection Program follows the National Infrastructure Protection Program.

For added resiliency, Riverside has portable transformers and switch gear on hand in the event there is a failure in any of their 14 substations. In the event of equipment failure, these portable units are temporarily installed and operated while a new replacement unit is ordered from the manufacturer.

This process may be a model for other POUs to follow.

H. Timeline for Implementation

According to the Joint Proposal, a utility would complete an initial draft of its mitigation plans within eighteen (18) months from the effective date of the guidelines. The utility is allowed 27 months to obtain third-party verification of the mitigation plans. Each utility is directed to meet its obligations within thirty (30) months of the effective date of the guidelines/Joint Proposal.

SED staff advises that all Security Plans be completed within 12 months of the adoption of this rulemaking by Commission Decision.

- A preliminary assessment of priority facilities is due to CPUC within 6 months of decision approval;
- A draft of the Distribution Security Plan is due for SED RASA review and approval within 12 months of decision approval.
- Within 15 months from decision approval, the publicly owned utilities shall provide CPUC with notice of plan adoption by way of copy of signed resolution, ordinance or letter by a responsible elected- or appointed official, or utility director.

Lastly, the Proposal should offer mention of some attempt to provide a cost estimate for annual expenses to support physical security efforts.

I. Additional Reporting

The recent SED White Paper produced as part of this proceeding discussed current reporting programs for physical security incidents. In particular it compared the U.S. Department of Energy's OE-417 reliability incident reporting program with insurance industry practices.

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, it is recommended that Utilities shall provide copies of OE-417 reports submitted to the U.S. Department of Energy (DOE) to the Director of the Safety and Enforcement Division and the Energy Division within two weeks of filing with DOE.

These utilities shall also submit an annual report by March 31 of the following year reporting physical security incidents that result in any utility insurance claims, providing information on incident, location, impact on infrastructure, and amount of claim.

J. Conclusion

One of our findings based on this proceeding is that California utilities do have effective physical security programs in place for critical assets at the transmission level. While there is always room for improvement, there is no significant reason that California utilities need to greatly increase spending for or begin new initiatives to address physical security of the distribution system.

However, this process has revealed a lack of transparency or justification provided for investments in the current utility physical security programs. There is evidence to suggest that implementation of relatively standardized security measures may reduce costs by preventing incidents of metal theft, one of the major vulnerability for distribution substations. The Sacramento Municipal Utility District presented information about how it recently reduced physical security incidents tenfold in two years at a marginal cost.

Our recommendations are intended to build upon the Joint Proposal and provide the Commission and the public with additional transparency whereby the effectiveness of physical security programs will be apparent without sacrificing the security of the electric grid.

The eventual Mitigation Plans envisioned by this process could include a mix of strategies: hardening of physical assets, increased security monitoring measures, or actions and programs to increase the resilience of the distribution network in the event of an adverse incident. It would be up to each utility to identify a cost-effective and optimal protection plan.

SED RASA is encouraged by this cooperative effort, and finds the Joint Proposal to be a workable approach to assuring California energy users that the utilities and the Commission are serious about safeguarding these important assets.

While generally supportive of the Joint Proposal, SED RASA recommends some additional provisions and considerations, along with the flexibility that would accommodate inherent differences between IOUs and POUs.

These proposed modifications to the Joint Proposal are meant to:

- Clarify Commission oversight authority and access to documentation;
    - The Distribution Security Program and Mitigation Plans should be subject to review and approval by Safety & Enforcement Division.
    - Failure to adhere to the compliance process may subject utilities to SED sanctions or penalties under current regulations.

    - Publicly owned utilities will not need to provide Mitigation Plans to the Commission, but should show compliance via formal adoption by their respective governing boards.

- Protect against unauthorized access to Confidential or Security-Sensitive Information;
    - While endorsing the Proposal's Reading Room approach as an interim measure for providing access, RASA emphasizes that in cases where the Commission is investigating an incident – whether it is already defined in our regulations or a new aspect, such as

physical or cyber attack, access to records shall be proved at the Commission's demand, not at the convenience of the utilities.

- Augment the criteria that utilities propose to use for determining "priority assets" that are subject to the Security Program
    - Adding consideration of assets that provide electric service to "essential customers" and especially vulnerable populations.
- Better define the criteria for third-party verification of the Distribution Security Programs and Mitigation Plans, and;
- A more expedited time table for utilities to provide an assessment of their systems and the approval of plans for compliance with this new program.
    - A preliminary assessment of priority facilities is due to CPUC within 6 months of decision approval;
    - A draft of the Distribution Security Plan is due within 12 months of decision approval.
    - Within 15 months from decision approval, the publicly owned utilities shall provide CPUC with notice of plan adoption by way of copy of signed resolution, ordinance or letter by a responsible elected- or appointed official, or utility director.
- Additional reporting requirements to fill in gaps in the CPUC's incident reporting policy.
    - Utilities should file with SED a copy of any OE-417 reports made to the US Department of Energy, and report annually on insurance claims associated with theft/vandalism at substations and control centers.

SED RASA's recommendations, as described above should be considered to augment and clarify the basic set of proposals embodied in the Utility Proposal.

###

SED Staff-proposed Ordering Paragraphs for Commission Consideration

IT IS ORDERED that:

1. Within twelve months from the date of Commission adoption of this Decision, Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty Utilities (collectively "the IOUs") shall each submit a summary of its Distribution System Physical Security Plan (Security Plan). The utilities shall provide full and unrestricted access to the Security Plan on utility property agreed to by the Safety and Enforcement Division, or its successor until such time that the Commission finalizes its rules for the handling, sharing, and inspection of confidential information.
2. Within twelve months from the date of Commission adoption of this Decision, the IOUs shall each provide the Commission a complete catalogue of distribution assets identified as serving essential customers and designated as priority assets;
3. Any and all California Electric Utility Distribution Asset Physical Security Plans shall conform to the requirements outlined within the Joint Utilities Proposal as modified by Commission Decision (rules and requirements collectively known as "security plan requirements").
4. Subsequent changes to the security plan requirements deemed beneficial and necessary, shall be enabled by one of the following: 1) Commission Decision; 2) Ministerially via public workshop and public notice and comment period; or via Tier 2 Advice Letter;
5. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty Utilities -- prior to submittal of each's Security Plan, shall have its respective plan reviewed by a third party entity other than the utility and having demonstrated appropriate physical security expertise.
6. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty Utilities shall document those third-party recommendations were accepted and declined, and provide justification supporting its decision.

This documentation shall be made available on utility property agreed to by the Safety and Enforcement Division, or its successor until such time that the Commission finalizes its rules for the handling, sharing, and inspection of confidential information.

7. Within twelve months from the date of Commission adoption of this Decision, the Publicly Owned Utilities in California (collectively, the "POUs") shall each submit to their governance authority (e.g., public Board of Directors or City Council) a Distribution Security Plan for adoption by. If the Publicly Owned Utility has an existing Security Plan that has been adopted by its public Board of Directors or City Council within the past three years, the requirement may be waved.
8. Within 15 months from the date of Commission adoption of this Decision, the publicly owned utilities shall provide notice of plan adoption by way of copy of signed resolution or letter by a responsible elected- or appointed official, or utility director. In the event that there has been some delay and adoption has not been completed, POUs shall provide the Commission with a notice informing of the nature of the delay and an estimated date for adoption.
9. Publicly Owned Utilities in California, prior of Security Plan adoption, shall have their plan reviewed by a third party. Such third party reviewer shall demonstrate qualifications as specified above in Ordering Paragraph 5. Such third party reviewer may be another governmental entity within the same political subdivision, so long as the entity can demonstrate appropriate expertise, and is not a division of the publicly owned utility that operates as a functional unit (i.e., a municipality could use its police department if it has the appropriate expertise.
10. Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty Utilities shall conduct a program review of their Security Plan and associated physical security program every five years after initial approval of the Security Plan by the Commission. A summary of the program review shall be submitted to the Safety and Enforcement Division within

30 days of Review completion. The utility shall provide full access to the Review on utility property agreed to by the Safety and Enforcement Division, or its successor.

11. Publicly Owned Utilities shall conduct a program review of their Security Plan and associated physical security program every five years after initial approval of the Security Plan by their public Board of Directors or City Council. Notice of such shall be provided to SED within 30 days of Plan adoption by way of copy of signed resolution or letter by a responsible elected- or appointed official, or utility director.
12. In the event of a major physical security event that impacts public safety or results in major sustained outages, all utilities shall preserve records and evidence associated with such event and shall provide the Commission full unfettered access to information associated with its physical security program and the circumstances surrounding such event.
13. The IOUs and POUs shall adhere to the SED Staff Response to Proposal described above, and shall fully comply with and carry out the provisions outlined within SED's recommended Six-step Security Plan Process.

###