STRAW PROPOSAL VERSION 2 (SDG&E)
R.15-06-009
Proposed Rules for Electric Utility Distribution System Security Assessments

PART 1:
INTRODUCTION

Purpose

The purpose of this initial proposal is to conceptually address the physical security risks to the distribution systems of electrical corporations. The eventual goal is to be in compliance with Senate Bill 699.[1]

Applicability

This proposal is intended to apply to electric utilities subject to the jurisdiction of the California Public Utilities Commission (Commission). Facilities subject to the California Independent System Utility's operational control and/or subject to FERC Reliability Standard CIP-014-2 or its successors are exempt from these rules.

General

This proposal is intended to implement a risk management approach with appropriate consideration for the resiliency, impact, and cost of steps to be taken to address the physical security risks to electrical distribution facilities. 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.

PART 2
RISK BASED DISTRIBUTION SECURITY PLANNING AND STANDARDS

At risk or "Covered" electric distribution facilities will be secured by:

- Establishing prioritized tiers of substations/infrastructure to protect, and
- Establishing risk based physical security standards for those tiers

Electric distribution facilities will be subject to an initial internal screening to determine whether they should be covered by this process, and if so, what Tier they are in. For purposes of this straw example, a utility's CIP-014-2 NERC sites could be Tier 0 (and thus already addressed, no

[1] (Ch. 550, Hill), as codified at California Public Utilities Code Section 364.

further action required), Tier 1 could encompass critical distribution facility sites or assets as determined by the utility (for example because the asset is required for cranking path/black start purposes or are located next to other sectors—like natural gas pipelines), and Tier 2 could include assets serving critical customers (government, military, emergency medical) or where physical threats could disrupt safe and essential public services, including safe drinking water. Each utility should determine which distribution assets belong in which Tier. Each utility would then determine which if any of these distribution assets may require additional security measures.

Prioritizing or sorting assets into tiers is appropriate because physical threats to substations and distribution assets depend on various factors. A predominant one is their location. For instance, electric distribution facilities located next to other sectors—like natural gas pipelines or water supply facilities[2]—or supplying power to such assets may have a different threat profile, as might those located in high-crime areas. Other physical characteristics include geographical challenges in implementing physical-security measures, proximity to highways or roads, and whether the facility is located in a rural area, with limited support from law enforcement.

Risk-Based Performance Standards (RBPSs) may be used to identify the areas for which a facility's security will be examined, such as perimeter security, access control, and personnel surety. A performance standard specifies the outcome required, but leaves the specific measures to achieve that outcome up to the discretion of the regulated entity. In contrast to a design standard or a technology-based standard that specifies exactly how to achieve compliance, a performance standard sets a goal and lets each entity decide how to meet it. To meet the RBPSs, utilities are free to choose and implement whatever security programs or processes they deem appropriate, measures to meet the RBPSs based on the facility's circumstances, including its tier level, security issues and risks, physical and operating environments, and other appropriate factors, so long as they achieve the requisite level of performance in each applicable area. The level of performance necessary to satisfy each RBPS is dependent on a facility's risk-based tier level, wherein higher-tier facilities are expected to meet higher levels of performance than lower-tier facilities. The programs and processes that a utility chooses to implement to meet these standards will be described in their Electric Distribution Site Security Plan (EDSSP). The measures that a utility selects and describes in its EDSSP should be tailored not only to the Covered Facility's tier level and security issues but also to the type of facility and its physical and operating environments. The CPUC (or California Office of Emergency Service (Cal-OES) would be able to review the EDSSP, perhaps combined with an on-site inspection, if it wishes to

[2] Drinking water facilities are mentioned in SB 699, Sec 1(b):
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.

determine whether or not a Covered Facility has met the requisite levels of performance established by the RBPSs given the facility's risk profile.

Potential performance standards will be developed by each utility, on the basis of the Covered Facility, (including existing system resiliency), its security risks, and its security program.

The following are EXAMPLES of RPBS types that could be developed and are not meant to be binding or definitive:

(1) Restrict Area Perimeter and Site Assets. Secure and monitor the perimeter of the facility; Secure and monitor restricted areas or potentially critical targets within the facility;

(2) Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter;[3]

(3) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful;[4]

(4) Theft and Diversion. Deter theft or diversion;

(5) Sabotage. Deter insider sabotage and cyber sabotage, including by preventing unauthorized on-site or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, and other sensitive computerized systems;

(6) Response. Develop and exercise an emergency plan to respond to security incidents internally and with the assistance of local law enforcement and first responders;

(7) Monitoring. Maintain effective monitoring, communications, and warning systems.[5]

---

[3] May include (i) Measures to deter the unauthorized introduction of devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and (ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access.

[4] May include measures to: (i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas; (ii) Deter attacks through visible security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced-value targets; (iii) Detect attacks at early stages, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and (iv) Delay an attack for a sufficient period of time to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and response planning;

[5] May include: (i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and maintained; (ii) Measures designed to regularly test security systems, note and correct detected deficiencies, and record results and (iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

(8) Personnel. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and, as appropriate, for visitors with access to restricted areas or assets[6]

(9) Elevated or Specific Threats. Escalate the level of protective measures for periods of elevated threat; Address specific threats, vulnerabilities, or risks identified for the particular facility at issue;

(10) Significant Security Incidents and Suspicious Activities. Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

(11) Records. Maintain appropriate records.

PART 3
DISTRIBUTION SECURITY PROGRAMS

1. General

Each Utility should establish, update as needed, and follow a Distribution Security Program. At a minimum, the Distribution Security Program should include the following:

A process by which each Utility should identify which, if any, of its distribution substations and distribution control centers or other distribution facilities are its Covered Distribution Facilities for the continued delivery of safe and reliable electric service. In identifying which are its Covered Distribution Facilities and determining their priority, the Utility may consider, among other factors:

- Spare assets needed/available to restore facility
- System resiliency and/or redundancy with facility out of service
- Whether facility provides backup power supply to other key facilities
- Existing capacity constrained, limited restoration capabilities under peak conditions
- Shares common location with critical transmission and/or generation assets, and/or whether facility provides backup power supply to other key facilities (e.g., power plants, water supply, etc.)

Using the risk based performance standards approach, each Utility should develop and implement documented physical security plans to address the risks identified for each of their Covered distribution facilities. The physical security plans should include consideration of the reasonableness of the cost of any recommended physical security improvements, and may also include efforts, activities or improvements other than security enhancements to improve the reliable operation of the distribution grid.

[6] May include: (i) Measures designed to verify and validate identity; (ii) Measures designed to check criminal history or identify people with terrorist ties.

2. Frequency

Time intervals or other bases should be specified in the Distribution Security Program.

3. Records

Electronic or hard copy records of the Security Program implementation should be as specified in the Reliability Based Performance Standard. Recommended minimums:

- identification of its Covered Distribution Facilities.
- evaluation of the potential threats and vulnerabilities of a physical attack on each of its Covered Distribution Facilities.
- physical security plans covering each of its Covered Distribution Facilities.
- evaluation of the security plan.

Electronic or hard copy records should be retained for five (5) years. Records maintained under this Part are extremely confidential and should be maintained in a secure manner by the Utility. The records maintained by electrical corporations should be available for inspection at the electric corporations' headquarters by Commission staff upon request.

PART 4
COMISSION OR GOVERNING BOARD REVIEW

The Commission may review electrical corporations' Distribution Security Program; this review should take place at the electrical corporations' headquarters using a Reading Room Approach, or as mutually agreed. For publicly owned electric utilities and electrical cooperatives (POU/EC), the governing board of the POU/EC should determine that the third-party verification was performed accurately.

PART 5
Definitions applicable to this proposal

Secure-Protected Information: Confidential Information, the disclosure of which could negatively impact public safety or the safe and reliable operation of a Utility's system.

Distribution Substation: an electric power substation associated with the distribution system and the primary feeders for supply to residential, commercial, and industrial loads.

Distribution Control Center: a facility that has responsibility for monitoring and directing operational activity on distribution power lines and substations by distribution system operators.

Electric Cooperative: As defined in California Public Utilities Code Section 2776.

Electrical Corporation: As defined in California Public Utilities Code Section 218.

Covered Distribution Facilities: Those distribution substations, distribution control centers or other distribution facilities that are addressed in a Utility's Distribution Security Program.

Local Publicly Owned Electric Utility: as defined in California Public Utilities Code Section 224.3.

Utility: an electric Utility, including a Local Publicly Owned Electric Utility or Electric Cooperative

Reading Room Approach: A method for sharing Secure-Protected Information with the Commission. Secure-Protected Information should be available for inspection at the Utility's headquarters, or a mutually agreed-to location, by Commission staff upon request.