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.	R.15-06-009 (Filed June 11, 2015)

PACIFIC GAS AND ELECTRIC COMPANY'S (U39) FINAL SECURITY PLAN REPORT IN COMPLIANCE WITH DECISION 19-01-018

Mark Esguerra

Pacific Gas and Electric Company
PO Box 7442
San Francisco, CA 94120
Telephone: (415) 973-0358
E-mail: mark.esguerra@pge.com

Senior Director of Asset Strategy
PACIFIC GAS AND ELECTRIC COMPANY

Dated: July 12, 2021

Pacific Gas and Electric Company

Final Security Plan Report

Implementing Requirements of Senate Bill 699 and Rulemaking 15-06-009

7/12/2021

Table of Contents

List of Figures

List of Tables

1.0 Document Control

Plan Revision Log

Table 1: Log of revisions to the Final Security Plan.

Date of Changes	Section(s) with changes	Summary of Changes	Changes Made by
7/10/2021	All	Initial Release	Pedram Arani

Plan Review Log

Table 2: Log of reviews of the Final Security Plan.

Date of Review	Name of Reviewer	Summary of Findings

1. Executive Summary

In this report, Pacific Gas and Electric Company (PG&E) provides the California Public Utilities Commission (CPUC) with a Final Security Plan Report as mandated per Ordering Paragraph 1 of the Phase I Physical Security Decision in D.19-01-018 dated January 10, 2019 ("Decision"). The report is a public document providing transparency and public awareness for PG&E's efforts to ensure a physically secure distribution grid. The attachments to this report are confidential and contain sensitive information about the operation of PG&E's grid. The confidential portions of this report will be made available to the appropriate staff at the Commission and will be further detailed with an encrypted and cybersecure virtual meeting to ensure compliance with the Phase I Decision mandates in accordance with the Interim Trial Procedures set forth in the Safety Policy Division's letter dated December 4, 2020 (the Interim Trial Procedures).

Starting in 2019, PG&E initiated the Preliminary Assessment and Identification, which PG&E refers to as P-1, of our Distribution Assets and Distribution Control Centers using the seven listed criteria to identify facilities that may merit special protection and measures to lessen any identified risks and threats. The P-1 Preliminary Assessment and Identification process resulted in the identification of the sites listed in the Confidential Attachment P-1 using the joint utility identifying designators and further detailed by PG&E's internal methodology, which were reported to the CPUC as required by Ordering Paragraph 1.

The distribution assets identified in the P-1 Preliminary Assessment and Identification which merited special protection were subject to a further secondary Vulnerability Assessment process, PG&E refers to as P-2. P-2 determined if the existing mitigations (physical security mitigations, redundancies, or customer-owned generation) for each site were sufficient, or if there was a need for additional mitigation to reduce any identified risks and threats to acceptable levels.

Any distribution asset identified in the P-2 Threat and Vulnerability Assessment that needed additional mitigations has been listed in PG&E's Mitigation Security Plans, which PG&E refers to as P-3. Mitigation recommendations are commensurate with the threat and risk level for the listed sites using a risk management approach with various considerations detailed in the confidential attachments. PG&E hardens assets and builds in redundancies where it makes economic sense based on likely risk, cost, and impact. However, protecting against all threats to our distribution assets can be costly and impractical. That is why rapid recovery is often the most cost-effective and flexible resilience strategy.

In accordance with the decision mandates, PG&E's P-3 Mitigation Security Plans were reviewed by an unaffiliated third-party entity that has demonstrated appropriate physical security expertise. The Third-Party Review provided recommendations, which PG&E refers to as P-4. PG&E then documented the P-4 Third-Party Review recommendations in attachment P-5, of which PG&E accepted all.

Compiling the documents, actions and reports detailed above, PG&E then developed this Final Security Plan Report for submission to the California Public Utility Commission as required and enumerated in item #2 of the Order by July 10, 2021. This Final Security Plan Report consists of our P-1, P-2, P-3, P-4, and P-5 addendums. This report also includes a detailed narrative response to questions posed in items #13, #14, #15 and #16 of the Order. This Final Security Plan Report will be reviewed every five years after the Commission's review of the initial plan as required and enumerated in item #25 of the Order and described in Section 4.2 of this report. As is described in Section 8 of this report, submission of this final security plan report constitutes PG&E's Step 3 of SED RASA's six step process described in Section 6.1 of the Decision.

2.0 Introduction & Background

As a result of the April 2013 rifle attack combined with the August 2014 burglary taking place in PG&E's Metcalf Substation, which is located south of San Jose, the CPUC made changes to the Public Utility Code § 364(a) addressing the vulnerability of electrical supply facilities to physical security threats. Since the approval of Senate Bill (SB) 699 in September 2014 the Commission issued an Order Instituting a Rulemaking to establish policies, procedures, and rules for the regulation of physical security risks to the electric supply facilities of electric utilities consistent with the Public Utility Code § 364 (Phase I). SB 699 amended Public Utility Code § 364 and required the Commission to develop rules for addressing physical security risks to the distribution systems of electrical corporations. The Commission held its initial prehearing conference on October 2015, which through Commission rulings, workshops, and other regulatory considerations, culminated into the Phase I Physical Security Decision.

To meet the requirements of SB 699, the Commission conducted four physical security workshops in the 2017-18 timeframe. In connection with these four workshops, a technical working group was formed by the parties which submitted the Joint Utility Proposal to provide guidance for compliance with Public Utility Code § 364. The Joint Proposal described how a utility should establish a Distribution Substation and Distribution Control Center Security Program which, among others, consisted of the following sections: P-1 Identification of distribution facilities, P-2 Assessment of physical security risk on distribution facilities, P-3 Development and implementation of security plans, P-4 Verification. Finally, the Decision ordered the Joint Utilities to prepare and submit to the Commission a Final Security Plan Report of all applicable facilities by July 10, 2021.

3.0 PG&E's Assets

PG&E, incorporated in California in 1905, is one of the largest combined natural gas and electric energy companies in the United States. PG&E provides electric service to approximately 16 million people throughout a 70,000 square-mile service area in northern and central California. PG&E serves over 5 million customer accounts via over 106,000 circuit miles of electric distribution lines which house 760 distribution substations. The image below outlines PG&E's service area.

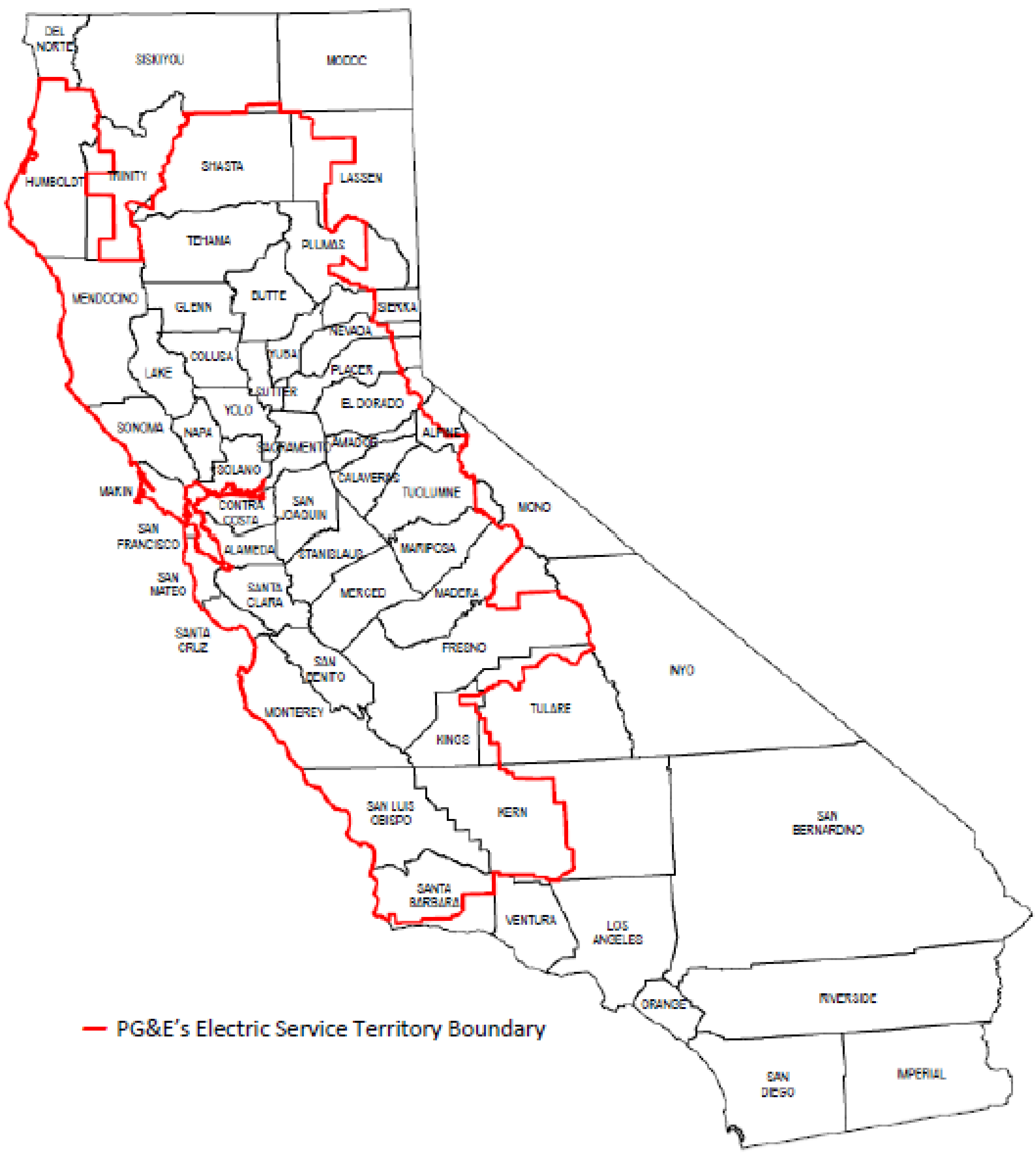

Figure 1: PG&E service area superimposed over the State of California county map.

4.0 Distribution Security Plan Contents and Management

This section of the report will address the Decision requirements, plan ownership and management by PG&E.

4.1 Requirements and Structure

The following table describes the requirements of the Final Security Plan as identified in the Ordering Paragraphs of D.19.01.018 and where detail can be found in this document to meet the specific requirement outlined. This table only reflect the Ordering Paragraphs that apply to the creation and submission of PG&E's Final Security Plan. The full list of Ordering Paragraphs and applicability to the company's Final Security Plan can be found in Attachment 6.

Table 3: Decision Requirements and Corresponding Plan References

Ordering Paragraph #	Description of the Ordering Paragraph	Corresponding Section in Plan
2	Within 30 months of this decision being adopted, Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall submit each utility's Final Security Plan Report.	Entire Document
5	All California Electric Utility Distribution Asset Physical Security Plans shall conform to the requirements outlined within the Joint Utility Proposal, as modified by this decision (rules and requirements collectively known as "security plan requirements").	See General Methodology in Section 8.0
6	The Investor Owned Utilities and Publicly Owned Utilities shall adhere to the Safety and Enforcement Division's Six-step Security Plan Process.	See General Methodology in Section 8.0
7	The Six-step Plan Process consists of the following: Assessment; Independent Review and Utility Response to Recommendations; Safety and Enforcement Division Review (for Investor Owned Utilities s); Local Plan Review (for Publicly Owned Utilities); Maintenance and Plan overhaul/new review.	See General Methodology in Section 8.0
8	Subsequent changes to the security plan requirements deemed beneficial and necessary, shall be enabled by one of the following: 1) Commission Resolution or Decision; 2) Ministerially, by Safety and Enforcement Division (or successor entity) director letter.	N/A for this document
9	In carrying out any future changes to the security plan requirements, Safety and Enforcement Division shall confer with utilities about any recommended modifications to the plan requirements.	N/A for this document

Ordering Paragraph #	Description of the Ordering Paragraph	Corresponding Section in Plan
10	Prior to the submittal of the Security Plan, Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall each have their respective plan reviewed by an unaffiliated third-party entity.	Section 8.4
11	The unaffiliated third-party reviewer shall have demonstrated appropriate physical security expertise.	Section 8.4
12	California electric utilities shall, within any new or renovated distribution substation, design their facilities to incorporate reasonable security features.	Section 5.0
13	Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement an asset management program to promote optimization, and quality assurance for tracking and locating spare parts stock, ensuring availability, and the rapid dispatch of available spare parts.	Section 6.2
14	Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement a robust workforce training and retention program to employ a full roster of highly-qualified service technicians able to respond to make repairs in short order throughout a utility's service territory using spare parts stockpiles and inventory.	Section 6.3
15	Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement a preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately.	Section 6.1
16	Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement a description of Distribution Control Center and Security Control Center roles and actions related to distribution system physical security.	Section 7.0
17	Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall each document all third-party reviewer recommendations, and specify recommendations that were accepted or declined by the utility.	Section 8.4
18	Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall each provide	Section 8.4

Ordering Paragraph #	Description of the Ordering Paragraph	Corresponding Section in Plan
	justification supporting its decision to accept or decline any third-party recommendations.	
22	Prior to Security Plan adoption, Publicly Owned Utilities in California shall have their plan reviewed by a third party.	Section 8.4
23	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).	Section 8.4
25	Pacific Gas and Electric Company, San Diego Gas & Electric Company, Southern California Edison, PacifiCorp, Bear Valley Electric Service, and Liberty CalPeco shall conduct a program review of their Security Plan and associated physical security program every five years after Commission review of the first iteration of the Security Plan.	Section 4.2
26	A summary of the program review shall be submitted to the Safety and Enforcement Division within 30 days of review completion.	Section 4.2
31	The utilities shall submit an annual report by March 31 each year beginning 2020, reporting physical incidents that result in any utility insurance claims, providing information on incident, location, impact on infrastructure and amount of claim. The insurance claim disclosure reporting, as described in this decision, should be included within a utility's broader annual Physical Security Report to the Commission due every March 31, beginning in 2020.	N/A for this document; Submitted annually by March 31.

Ordering Paragraph #	Description of the Ordering Paragraph	Corresponding Section in Plan
32	As appropriate, the requirements set forth in Phase I of this proceeding shall apply to Alameda Municipal Power, City of Anaheim Public Utilities Department, Azusa Light and Water, City of Banning Electric Department, Biggs Municipal Utilities, Burbank Water and Power, Cerritos Electric Utility, City and County of San Francisco, City of Industry, Colton Public Utilities, City of Corona, Eastside Power Authority, Glendale Water and Power, Gridley Electric Utility, City of Healdsburg Electric Department, Imperial Irrigation District, Kirkwood Meadows Public Utility District, Lathrop Irrigation District, Lassen Municipal Utility District, Lodi Electric Utility, City of Lompoc, Los Angeles Department of Water & Power, Merced Irrigation District, Modesto Irrigation District, Moreno Valley Electric Utility, City of Needles, City of Palo Alto, Pasadena Water and Power, City of Pittsburg, Port of Oakland, Port of Stockton, Power and Water Resources Pooling Authority, Rancho Cucamonga Municipal Utility, Redding Electric Utility, City of Riverside, Roseville Electric, Sacramento Municipal Utility District, City of Shasta Lake, Shelter Cove Resort Improvement District, Silicon Valley Power, Trinity Public Utility District, Truckee Donner Public Utilities District, Turlock Irrigation District, City of Ukiah, City of Vernon, Victorville Municipal Utilities Services, Anza Electric Cooperative, Plumas-Sierra Rural Electric Cooperative, Surprise Valley Electrification Corporation, and Valley Electric Association.	N/A for this document
33	This proceeding shall remain open so that the Commission may address the issues presented in Phase II of this proceeding.	N/A for this document

4.2 Plan Management and Ownership

Ordering Paragraph 25 of the Decision stipulates that the Investor Owned Utilities (IOU) conduct a program review of their Security Plan and associated physical security program every five years after Commission review of the first iteration of the security plan. The deadline to submit the second iteration of this Final Security Plan is July 9, 2026. All reviews and revisions to the plan will be tracked utilizing the Document Control section of the report. Per OP 26 of the Decision, a summary of the program review shall be submitted to the Safety and Enforcement Division within 30 days of review completion, or August 9, 2026.

5.0 New Substation Construction

Per ordering paragraph 12 of the Decision, PG&E will design all new or renovated distribution substations to incorporate reasonable security features in line with the methodology described in section 8.3 of this report.

6.0 Substation Asset Management Programs

This section covers items that pertain to distribution substation physical security and maintenance.

6.1 Substation Security Inspection Program

Ordering Paragraph 15 of the Decision states that Utility security plans shall include a detailed narrative explaining how the utility is taking steps to implement a preventative maintenance plan for security equipment to ensure that mitigation measures are functional and performing adequately. PG&E has developed preventative maintenance plans which utilize time-based and condition-based activities to ensure security equipment functions as designed. A summary of the security maintenance program for each of the Covered Distribution Facilities is included in the P-3 Mitigation Security Plans of each facility. These materials are confidential and will be made available in accordance with the Interim Trial Procedures

6.2 Critical Spare Inventory Management

Ordering Paragraph 13 of the Decision requires the utility security plan to include a detailed narrative explaining how the Utility is taking steps to implement an asset management program to promote optimization, and quality assurance for tracking and locating spare parts stock, ensuring availability, and the rapid dispatch of available spare parts. PG&E's Substation Asset Strategy manages capital emergency materials which include transformers, breakers, regulators, and mobile transformers for emergency responses. Substation Asset Strategy also maintains spare transformers in some of PG&E's substations. For example, there are three single phase units for a transformer bank with a fourth (spare) phase that could be cut-in to replace a failed transformer phase within 4-8 hours. Spare parts such as bushings, insulators, etc., are stocked at various locations. PG&E has identified strategic locations where spare inventory is maintained. These materials are confidential and will be made available in accordance with the Interim Trial Procedures.

6.3 Asset Replacement/Repair

Ordering Paragraph 13 of the Decision requires the utility security plan to include a detailed narrative explaining how the Utility is taking steps to implement a robust workforce training and retention program to employ a full roster of highly-qualified service technicians able to respond to make repairs in short order throughout a utility's service territory using spare parts stockpiles and inventory.

PG&E utilizes a 36-month Electrician and a 30-month Electrical Technician apprenticeship program to train our substation workforce to the highest standard. The apprenticeships consist of a blend of Instructor-led training, on-the-job training, and work experience. The instructor led training is designed to develop proficiency with substation equipment and procedures. This training includes but is not limited to electrician's math and principles, reading and understanding schematic diagrams, circuit breakers, transformers, load tap changers, air switches (manual and motor operated), rigging, and grounding. The on-the-job training that the apprentices are required to complete is designed and scheduled to reinforce learnings from instructor-led courses recently completed. The on-the-job training consists of mandated hours of work on specific tasks, including wiring from schematics, equipment installation, commission testing, rigging, grounding, installing conduit and bus work, pulling wire, as well as operating power tools and equipment safely.

To maintain our knowledge base, each employee is profiled with a training plan that correlates with their current job assignment. We provide refresher training to reinforce critical skills such as switching and grounding on a periodic basis. Ongoing refresher training is provided where applicable, which includes (but is not limited to) First Responder Evidence Preservation, Standards of Conduct, and Cyber and Physical Security Standards. New procedures, test equipment and technologies are evaluated to determine if training is required and when required, focused training is delivered.

In addition, we have a Knowledge and Skills program that is designed to assess each journeyman to ensure they perform critical tasks according to the procedures. This is done on a periodic basis and on a variety of critical tasks. Employees that are not able to demonstrate competence are retrained to ensure a highly skilled workforce.

7.0 PG&E's Distribution Control Center

OP 16 of the Decision stipulates that the utility security plans will include a detailed narrative explaining how the utility is taking steps to implement a description of Distribution Control Center and Security Control Center roles and actions related to distribution system physical security. As part of the development of PG&E's P-3 Mitigation Security Plan, PG&E developed Distribution Control Center roles and responsibilities which clearly outline the actions operators should take when they witness or receive reports of hostile, criminal, or suspicious activity. Similarly, as part of PG&E's P-3 Mitigation Security Plan, PG&E developed two security procedures that describe the process for PG&E's Corporate Security Department's Security Control Center to manage and respond to reported situations or alarms. Additional details on the Distribution and Security Control Centers are confidential and will be made available to the appropriate staff at the Commission in accordance with the Interim Trial Procedures.

8.0 PG&E'S Distribution Security Program

Section 4 of the Decision outlines the Joint Utility Proposal which describes how a utility should establish Distribution Substation and Distribution Control Center Security Program. This program consists of the following seven steps: 1) Identification of distribution facilities, 2) Assessment of physical security risk on distribution facilities, 3) Development and implementation of security plans, 4) Verification, 5) Record keeping, 6) Timelines and 7) Cost recovery. Each step is described in more detail in sections 4.1 through 4.7 of the Decision. Sections 8.1 through 8.7 utilize a similar structure to share PG&E's methodology and results in following the Joint Utility Proposal.

Section 6.1 of the Decision outlines the CPUC's Safety and Enforcement Division's Risk Assessment and Safety Advisory's (SED RASA) recommended six-step procedure for carrying out the new physical security plan requirements for the utilities' distribution assets. The six steps are:

1. Assessment: Drafting of a plan, addressing prevention, response, and recovery, which could be prepared in-house or by a consultant, and which shall include proposed and recommended mitigation measures.
2. Independent Review and Utility Response to Recommendations: Proposed plan would be reviewed and by an 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 that assess and appraise the appropriateness of the risk assessment, proposed mitigation measures, and other plan elements. A utility 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.
3. SED Review (for IOUs only): Final plan report would be reviewed by the CPUC SED (recurring every five years) so as to determine whether it is in compliance with regulatory requirements, and eligible to request funding for implementation. Upon five years from the date of adoption, a utility would be required to have any revised or original plan updated and repeat the review 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 review process may be impracticable or unduly burdensome. Non-compliance could result in an enforcement action, potentially resulting in sanctions and/or penalties as provided by PU Code Sec. 364(c). An SED finding of compliance would render IOUs eligible to request funding for appropriate physical security needs identified by IOUs; project expenditures would be tracked in a memorandum account and subject to reasonableness review in the GRC.
    a. Plan Review (for POUs only): Final plan report would be deemed adequate (recurring every five years, and eligible for same exemption request process made available to the IOUs) 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 the Governor's Office of Emergency Services (CalOES) and Federal Emergency Management Agency (FEMA) standards and receives their endorsement.)

4. Adoption (for POUs only): Reviewed plan would be submitted to the appropriate regulatory oversight body (local governance body) for review and greenlighting (adoption). Step 4 should include funding to implement the plan.
    a. Notice (for POUs only): Provide CPUC with official notice (ideally including a copy of a resolution of the adopted plan action.
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.
6. Repeat Process: Plan overhaul and review every five years.

The completion and transfer of this report to SED constitutes PG&E's submission of the final plan report for SED Review and completion of Steps one through three.

8.1 Identification

Section 4.1 of the Decision details the identification of distribution facilities as outlined in the Joint Proposal describes how a utility should establish a Distribution facility (substations) and Distribution Control Center Security Program. PG&E identified a potential of 239 distribution facilities and were evaluated prior to providing PG&E Corporate Security the distribution facilities for Threat and Vulnerability Assessments and Mitigation Security Plans. PG&E referred to Section 4.1 – Identification and Section 4.2 collectively as P-1.

8.1.1 Identification Methodology

PG&E used the following criteria outlined in Section 4.1 to identify distribution assets to go through threat and vulnerability assessments as well as a mitigation plan for selected facilities:

1. Distribution Facility necessary for crank path, black start or capability essential to the restoration of regional electricity service that are not subject to the California Independent System Operator's (CAISO) operational control and/or subject to North American Electric Reliability Corporation (NERC) Reliability Standard CIP-014-2 or its successors;

2. Distribution Facility that is the primary source of electrical service to a military installation essential to national security and/or emergency response services (may include certain airfields, command centers, weapons stations, emergency supply depots);

3. Distribution Facility that serves installations necessary for the provision of regional drinking water supplies and wastewater services (may include certain aqueducts, well fields, groundwater pumps, and treatment plants);

4. Distribution Facility that serves a regional public safety establishment (may include County Emergency Operations Centers; county sheriff's department and major city police department headquarters; major state and county fire service headquarters; county jails and state and federal prisons; and 911 dispatch centers);

5. Distribution Facility that serves a major transportation facility (may include International Airport, Mega Seaport, other air traffic control center, and international broader crossing);

6. Distribution Facility that serves as a Level 1 Trauma Center as designated by the Office of Statewide Health Planning and Development; and

7. Distribution Facility that serves over 60,000 meters

8.1.2 Identification Results – List of Covered Facilities

PG&E identified a potential of 239 distribution facilities that were evaluated prior to providing PG&E Corporate Security the distribution facilities for Threat and Vulnerability Assessment and Mitigation Security Plan. A summary of those facilities is confidential. The confidential portions of this report will be made available to the appropriate staff at the Commission in accordance with the Interim Trial Procedures.

8.2 Assessment

Section 4.2 of the Decision details the Assessment of distribution facilities as outlined in the Joint Proposal. This step includes the evaluation of the potential risks associated with a successful physical attack on a facility and whether existing grid mitigations address those identified risks. PG&E applied the assessment methodology to all 239 facilities as requested by CPUC staff. PG&E referred to Section 4.1 – Identification and Section 4.2 collectively as P-2.

8.2.1 Assessment Methodology

The identified distribution facilities were assessed for exclusion from physical security assessment and mitigation plan based on some of the recommendations outlined in Section 4.2 of the Proposed Decision. The recommendations applied were:

1. The existing system resiliency and/or redundancy solutions;
2. The availability of spare assets to restore a particular load;
3. The existing physical security protections to reasonably address the risk;
4. The potential for emergency responders to identify and respond to an attack in a timely manner;
5. Location and physical surroundings
6. History of criminal history activity at the Distribution Facility and in the area;
7. The availability of other sources of energy to serve the load;
8. Requirements served by the load.

The outcome of this pre-assessment indicated that only five of PG&E distribution facility did not meet one or more of the factors.

8.2.2 Assessment Results

The following 5 substations were identified as requiring Mitigation Security Plans. Due to the restricted nature of this information, PG&E has provided the below code names of the substations. Confidential details like this will be made available to the appropriate staff at the Commission in accordance with the Interim Trial Procedures.

List of Distribution Facilities:

1. Sub 68
2. Sub 185
3. Sub 186
4. Sub 189
5. Sub 190

8.3 Mitigation Plan

Section 4.3 of the decision details the requirement of each Operator to develop and implement a mitigation plan for Covered Distribution Facilities. For PG&E this portion of the Decision was covered by the combination of P2 – Threat & Vulnerability Assessment and P3 – Mitigation plan.

8.3.1 Threat & Vulnerability Assessment.

Onsite security assessment and security analysis was performed using a Design Basis Threat ("DBT") methodology, which is recommended within Senate Bill 699. SB 699 amended Public Utilities Code 364 and requires PG&E to identify and develop a mitigation plan to reduce physical security risks to their distribution systems. To address the risk of a long-term outage due to a physical attack, PG&E has developed a mitigation plan to reduce physical security risks at the identified substations.

Under SB 699, PG&E has discretion to select the specific security measures that are most appropriate for the identified substation. The current categories for the identified substation's security conditions are summarized below:

- Threat: Low Threat level. Based on interviews with staff and the assessment team participants there is no known record of any significant security incidents or evidence of sophisticated or motivated aggressors in the local area or region with the intention of destroying or significantly damaging the distribution operations or infrastructure at the identified substations. The threat level is, therefore low based on the Design Basis Threat analysis.
- Vulnerability: Low to Moderate Vulnerability level. These sites are generally fully enclosed buildings located in an urban environment and are highly visible with two major roadways directly adjacent to the sites. The main substation structures are accessible in some areas by foot. Physical security measures are in place to reduce vulnerability by deterring access to the substation structures in the form of an ornamental metal fence and temporary chain-link fence, the building façade itself, locked doors and gates. Access to these substations by small to medium sized vehicles would be delayed by the existing security measures. Some of the sites are occupied 24x7, monitored continuously, but there are no automated detection and assessment capabilities. Others are monitored by PG&E's security control center. The substations are most vulnerable to a forced entry adversarial attack by sophisticated or a highly motivated aggressor(s). The vulnerability level is therefore low to moderate based on the Design Basis Threat analysis.
- Physical Security Measures: Moderate Physical Security protections. Security measures are in place to hinder access to the building structures in the form of fences, secured gates and locked doors. Protective measures in place are generally consistent with industry practices, but vulnerabilities do exist, as the existing security measures may be bypassed by a motivated aggressor.

Engineering and operations personnel along with security subject matter experts, identified that there are three critical distribution related assets or asset types at the identified substations.

The considerations provided in this report are provided to enhance and strengthen PG&E's security program at the identified substations. Additional physical security structural enhancements, technology and security awareness programs will be considered to cover each identified critical assets or key operational elements using seven fundamental security requirements: Deterrence, Detection, Assessment, Communications, Delay, Response and Recovery.

The identified substations have unique characteristics and challenges when it comes to physical security. Upon analysis, there were several characteristics that increase the risk of adversarial actions at these locations. They are:

- Social Economic Demographics: High-crime area, shelterless, vagrancy and drug use in areas directly adjacent to the site.
- Geography: An urban environment surrounded by other business and downtown residences. These hotels and residences are directly adjacent to the properties, which increases the potential for hostile surveillance and routine public activity near the sites.
- Historical Issues: Two (2) previous accidental equipment-initiated fires, several acts of vandalism and trespassing, and one (1) nearby aggravated assault (stabbing).
- Site Characteristics: Lack of set-back distance from the public street and sidewalks decreases delay features and increases visibility and accessibility for potential offenders.
- Physical Protection System Vulnerabilities: Minimal detection, assessment and communication capabilities exist at the site. Several delay barriers and access points have potential gaps.
- Security Awareness: During the site visit, there were several doors propped open by contractors working at the site. In addition, two security devices have been altered to prevent proper operability.

The threats assessed per SB-699 were based on the SB 699 Design Basis Threat (DBT) Joint Utility Working Group and Electricity Information Sharing & Analysis Center (E-ISAC) Design Basis Threat Methodology. Per guidance documentation provided by these groups, PG&E determined the most likely threats for the applicable sites.

8.3.2 Mitigation Plan

Based on site-specific Threat and Vulnerability Assessments, PG&E utilized the design basis methodology to evaluate the potential need to enhance existing physical security countermeasures. Each mitigation plan was written with consideration of location, surrounding terrain, unique substation characteristics, existing resiliency, defined risks, possibility probability of successful attacks, and the proposed solutions ability to mitigate and respond to potential physical attacks effectively. PG&E's mitigation plans include a project plan to implement countermeasures with a demonstrated capability to effectively deter, detect, delay, assess, communicate, respond, and recover.

PG&E considered enhanced physical security controls for sites as a whole and considered the need for increased security countermeasures for the assets deemed most critical to site function. As a general statement, each mitigation plan includes overarching site security and spot solutions based on the asset types and inherent vulnerabilities. Physical access controls and automated alarming capabilities facilitate alarm assessment and appropriate response measures are effectively and efficiently deployed.

PG&E defines the key elements of each mitigation plan as follows:

- Deter – visible physical security countermeasures that are installed to discourage a potential adversary from attacking through means of fear or doubt, due to the risk of being identified and/or apprehended (either during or after the attack).
- Detect – physical security countermeasures installed to identify unauthorized intrusion or potential nefarious activity and provide adversary notification/annunciation.
- Assess – the process of evaluating the legitimacy of an alarm or suspicious activity; if an undesired physical security event is developing, making the determination that immediate communication and response are necessary.
- Delay – physical security countermeasures installed, which slow a potential adversary's access to an asset or critical components, enabling response to an attack.
- Communicate – notification systems (or methods) utilized to inform response personnel of an alarm or suspicious activity; or alerting a potential adversary that they are being monitored.
- Response - the immediate security actions taken after detection and assessment of a potential attack designed to interrupt, apprehend, or implicate an adversary.
- Recovery – the ability to get back to normal operations after an incident or attack.

8.3.3 Results

The content of P2 – Threat & Vulnerability Assessments and P3 – Mitigation plans are confidential and will be made available to the appropriate staff at the Commission in accordance with the Interim Trial Procedures.

8.4 Verification

Section 4.4 of the Decision describes the requirement that each Operator select an unaffiliated third party with appropriate experience to review the Identification and Assessment evaluations and Mitigation Plans performed and developed by the Operator. Following the evaluation of the Identification and Assessment evaluations and Mitigation Plans each Operator is required to modify these documents to be consistent with the recommendations or document its reasons for doing so. Within this section, PG&E will include subsections detailing the qualifications of the unaffiliated third parties, high-level findings, and other relevant information.

8.4.1 Qualifications

PG&E used two unaffiliated third parties to review the Identification and Assessment evaluations and Mitigation Plans performed and developed by PG&E. The first evaluator provided review and suggested modifications of the Identification and Assessment evaluations; the second evaluator provided review and suggested modifications to the Mitigation Plans[1]. The names and identifying descriptors of the evaluators have been purposefully removed. Names and additional biographical information on the two evaluators is included in the confidential attachment P-4.

8.4.1.1 Evaluator 1 Qualifications

8.4.1.1.1 Electrical Industry Experience

Evaluator 1 has been employed in the electrical sector since 1973. Beginning their career as an apprentice lineman, they worked on numerous transmission power line and substation construction projects across the North American electrical grid. They joined the hot stick and barehand transmission live line maintenance team at a transmission and generation utility in Arizona (1982-1990). They became a power system operator in the utility's System Control Center in 1990. Among various operational duties, they were responsible for monitoring and responding to security breaches at electrical facilities. They transferred to the utility's Information Technology department in 1998 and were responsible for electronic and physical security for operational cyber systems located around the utility's service territory. Evaluator 1 accepted their final role at the utility in 2008 and managed the Power Trading and Scheduling department.

After taking early retirement from the utility in February 2011, evaluator 1 began working at the Western Electricity Coordinating Council (WECC) on the Critical Infrastructure Protection (CIP) audit team as a Senior Compliance Auditor. They participated in and led numerous audits and other investigations during this time. When the CIP-014-2 Standard was approved by FERC in 2015, evaluator 1 led the WECC effort to establish the CIP-014-2 audit approach and provided significant outreach to Transmission Owners (TO) and Transmission Operators (TOP) to support compliance with the new Standard. Once CIP-014-2 became mandatory and enforceable in

[1] Mitigation Plan consists of PG&E's P2 – Threat & Vulnerability Assessment and P3 – Mitigation plan.

October 2015, they became the audit team lead for compliance with Requirements R1, R2, and R3 and supported the R4, R5, and R6 audit teams, as needed, during TO and TOP audits.

Evaluator 1 retired from WECC in November 2019 and immediately joined Guidehouse as a Managing Consultant and is presently employed as an Associate Director. During their time at Guidehouse, they have worked on several CIP-014 documentation review and physical security projects for clients across the North American electrical grid. Evaluator 1 is not affiliated with PG&E or the CPUC in any manner, other than by a contractual basis through Guidehouse to perform work for PG&E as an independent and unaffiliated contractor. They also meet the qualification requirements of D.19-01-018 Section 6.4 based on their extensive electrical sector expertise and prior work with CIP-014-2 and other physical security audits, which was approved by WECC and NERC. The final required qualification is realized by evaluator 1's current list of globally recognized cyber security and physical security certifications.

8.4.1.1.2 Relevant Education & Certifications

Evaluator 1 earned a Bachelor of Science degree in Computer Science from the University of Arizona and an MBA at the Eller College of Management – University of Arizona. Their Ph.D. in Organization and Management, with a specialization in Leadership, was conferred by Capella University in 2008.

Complementing their academic and professional qualifications, evaluator 1 holds relevant physical security certifications, as described in Section 6.4 of the Decision , which were awarded by ASIS International, a globally recognized community of security practitioners, who play significant roles to ensure electronic and physical security protections of various assets, information, and personnel across the 16 critical public infrastructure sectors. They also hold numerous operations, cybersecurity, auditing, project management, and risk management certifications, several of which are included in Table 1-1 below:

Table 4: Summary of evaluator 1's certifications.

Certifying Agency	Certification Description	Certification Number
ASIS Intl.	Physical Security Professional [PSP]	20077
ASIS Intl.	Certified Protection Professional [CPP]	20742
ASIS Intl.	Professional Certified Investigator [PCI]	21806
ISACA	Certified Information System Manager [CISM]	0300492
ISACA	Certified in Risk & Information Systems Control [CRISC]	1112935

ISACA	Certified Information System Auditor [CISA]	12103648
ISC^2	Certified Information Systems Security Professional [CISSP]	32233
NERC	Balancing & Interchange System Operator	BI200911009
PMI	Project Management Professional [PMP]	41619

8.4.1.2 Evaluator 2 Qualifications

8.4.1.2.1 Electrical Industry Experience

Evaluator 2 has been an associate director at Guidehouse since 2019 where they have done extensive work within the utility sector conducting threat vulnerability assessments and helping entities develop robust physical security programs. In their role in Guidehouse' s Energy, Sustainability, and Infrastructure segment evaluator 2 leads the assessment and development of business strategies, organizational structures, and business processes for utility clients. They assess and evaluate client business processes, internal controls, and overall enterprise risk and security. Upon evaluating these disciplines, evaluator 2 leads, designs, recommends, and facilitates process improvements throughout the energy market. Their broad physical security and leadership experience enables them to successfully manage multiple projects with differing timelines and budgets to ensure the delivery of cost-effective client solutions. They have demonstrated success in providing guidance on utility-level regulatory compliance, developing and implementing security programs to support continuous quality improvement, reducing enterprise risk, and promoting cross-functional collaboration. For 13 years prior to joining Guidehouse, evaluator 2 was a Manager of Physical & Cyber Security Audits & Investigations at the Western Electricity Coordinating Council (WECC), a regional regulator for the NERC Electric Reliability Office. They were responsible for a variety of related areas that include staffing, planning, and executing operations, audits, and developing and implementing a broad range of topics involving internal and external compliance training. They have held security management roles with two large investor-owned utilities prior to their service at WECC. Evaluator 2 has 30 years of experience in the coordination and implementation of security services.

8.4.1.2.2 Relevant Education and Certifications

Evaluator 2 earned their BA in Police Science from Ottawa University and their MBA at Northern Arizona University. They have also completed the ASIS International Security Executive Management Program at the Wharton School, University of Pennsylvania. Complementing their academic and professional qualifications, evaluator 2 holds relevant physical security certifications, as described in Section 6.4 of the Decision, which were awarded by ASIS International, a globally recognized community of security practitioners, who play significant roles to ensure electronic and physical security protections of various assets, information, and personnel across the 16 critical public infrastructure sectors. Their relevant certifications are included in the table below.

Table 5: Summary of evaluator 2's certifications.

Certifying Agency	Certification Description	Certification Number
ASIS Intl.	Physical Security Professional [PSP]	15782
ASIS Intl.	Certified Protection Professional [CPP]	14589
ASIS Intl.	Professional Certified Investigator [PCI]	16088

8.4.2 Results

This section of the report provides high level descriptions of the unaffiliated third-party review of PG&E's Identification and Assessment evaluations and Mitigation Plans. The documents outlining the results of the review are confidential and will be included in this final report's confidential attachment P-4. These confidential portions of the report will be made available to the appropriate staff at the Commission in accordance with the Interim Trial Procedures.

8.4.2.1 Identification Results

The unaffiliated third-party review of the Decision Section 4.1 Identification resulted in a set of suggestions that would improve the quality of the associated excel workbook and improve the efficiency of process moving forward. An updated workbook is included in this final report's confidential attachment P-1. Detailed descriptions are confidential and are included in this final report's attachment P-3.

8.4.2.2 Assessment Results

The unaffiliated third-party review of the Decision Section 4.2 Assessment resulted in a set of suggestions that would reduce the time needed to conduct the analysis. Detailed descriptions are confidential and are included in this final report's attachment P-3.

8.4.2.3 Mitigation Results

The unaffiliated third-party review of the Decision Section 4.3 Mitigation Plan resulted in a set of suggestions that would improve the quality of the plan as well as improve security commissioning in future plans. Detailed descriptions are confidential and are included in this final report's attachment P-3.

8.4.3 PG&E Response

A summary of all recommendations and PG&E's response to each recommendation are included in this final report's confidential attachment P-5.

8.4.3.1 Identification Response

PG&E accepted all recommendations from the unaffiliated third party related to the Decision Section 4.1 Identification portion of the order. When implemented, the unaffiliated third-party review resulted in the required review of an additional 10 distribution facilities resulting in a total of 249 reviewed facilities. A revised workbook is included in this final report's attachment P-1. A summary of those recommendations can be found in the confidential attachment P-4.

8.4.3.2 Assessment Response

PG&E accepted all recommendations from the unaffiliated third party related to the Decision Section 4.2 Assessment portion of the order. When PG&E applied the assessment to the additional 10 distribution facilities described in 8.4.3.1, PG&E did not identify the need for additional Threat and Vulnerability Assessments or Mitigation Plans. A summary of those recommendations can be found in the confidential attachment P-4.

8.4.3.3 Mitigation Response

PG&E accepted all recommendations from the unaffiliated third party related to the Decision Section 4.3 Mitigation portion of the order. A summary of those recommendations can be found in the confidential attachment P-4.

8.5 Record Keeping

Consistent with the JUP, electronic copies of this Distribution Security Program Implementation will be retained for not less than five (5) years. As such records are extremely confidential, these records will be maintained in a secure manner at the Operator's headquarters. The records maintained by an Operator will be available for inspection at its headquarters by Commission staff upon request.

These records will include, at a minimum:

1) The Operator's Identification of Distribution Facilities requiring further assessment;

2) Each Operator's Assessment of the potential threats and vulnerabilities of a physical attack and whether existing grid resiliency, customer-owned back-up generation and/or physical security measures appropriately mitigate the risks on each of its identified Distribution Facilities;

3) Each Operator's Mitigation Plans covering each of its Covered Distribution Facilities under Section 4;

4) The unaffiliated third-party evaluation of the Operator's Identification and Assessment evaluations and Mitigation Plans performed and developed by the Operator; and

5) If applicable, the Operator's documented reasons for not modifying its Mitigation Plans consistent with the unaffiliated third-party's evaluation.

8.6 Timeline

PG&E's Mitigation Plan's for the identified substations include short, medium, and long term recommended measures for each identified substation. Short term measures refer to mitigations that require between 1-2 years; medium term measures refer to mitigations that require between 3-4 years; long term measures refer to mitigations that will require between 5-8 years to implement. Estimated costs for these mitigation measures range from as little has $5,000 to more than $1 million. The Mitigation Plans are confidential and will be included in this final report's attachment P-3. These confidential portions of the report will be made available to the appropriate staff at the Commission in accordance with the Interim Trial Procedures.

8.7 Cost

The following describes PG&E's high level cost estimates and annual spend to implement the projects identified in Section 0 and the timelines included in Section 0. These costs do not include labor. Please note that although each substation has long lead time items, the majority of the suggested projects can be implemented in the medium and short time horizons.

Table 6: Summary of substation mitigation costs and long-lead timelines.

Substation	Total Cost	Implementation Long Lead Time Item
Substation 68	$4.137 Million	5-8 Years
Substation 185	$4.472 Million	5-8 Years
Substation 186	$4.037 Million	5-8 Years
Substation 189	$1.147 Million	5-8 Years
Substation 190	$1,150 Million	5-8 Years

Respectfully submitted,

By: *\/s/ Mark Esguerra*
Mark Esguerra

Pacific Gas and Electric Company
P.O. Box 7442
San Francisco, CA 94120
Telephone: (415) 973-0358
E-mail: mark.esguerra@pge.com

Senior Director of Asset Strategy
PACIFIC GAS AND ELECTRIC COMPANY

Dated: July 12, 2021