Docket:	A.17-04-010
Exhibit Number:	ORA-
Commissioner:	Liane Randolph
Admin. Law Judge:	Jessica T. Hecht
ORA Project Mgr.:	Ana Maria Johnson
ORA Expert Witness:	Cameron Reed

ORA
OFFICE OF RATEPAYER ADVOCATES

Office of Ratepayer Advocates

California Public Utilities Commission

Office of Ratepayer Advocates Testimony Regarding Safety and the Cybersecurity Risk of Pacific Gas and Electric Company's Application for a Certificate of Public Convenience and Necessity to provide Competitive Local Exchange Services

San Francisco, California
November 22, 2017

MEMORANDUM

This report was prepared by Cameron Reed of the Communications and Water Policy Branch of the Office of Ratepayer Advocates ("ORA") under the general supervision of Program & Project Supervisor, Ana Maria Johnson. Cameron Reed's statement of qualifications is presented in Attachment A to this testimony. ORA is represented in this proceeding by legal counsel Niki Bawa.

This testimony is comprised of the following chapters:

Chapter	Description
I	**Introduction**: An introduction to the issues covered in this testimony, including why addressing Cybersecurity risk is important.
II	**Summary of Recommendations**: A summary of recommendations addressing safety and Cybersecurity risk.
III	**Discussion:** A discussion covering how to define risk, Cybersecurity and safety practices, and how PG&E plans to mitigate its Cybersecurity risk.
IV	**Conclusion**: A conclusion recounting the main points presented within this testimony.

TABLE OF CONTENTS

Memorandum 1

Executive Summary 4

I. Introduction 6

II. Summary of Recommendations 8

III. Discussion 9

A. Network Security and Segmentation 10

B. Network Operations 12

C. PG&E's Business Plan 13

D. Fiber Cable in the Electrical Supply Space 14

IV. Conclusion 16

ATTACHMENTS

Attachment A: Statement of Qualifications and Experience 18

Attachment B: PG&E Response to ORA Data Request No. 1 19

Attachment C: PG&E Response to ORA Data Request No. 1, Question 14, Attachment 1 36

Attachment D: PG&E Response to ORA Data Request No. 1, Question 14, Attachment 2 40

Attachment E: PG&E Response to ORA Data Request No. 3 62

Attachment F: Excerpt from ORA Supporting Attachments in A.15-09-001 66

EXECUTIVE SUMMARY

On April 6 2017, Pacific Gas and Electric Company ("PG&E") filed Application 17-04-010 ("Application") with the California Public Utilities Commission ("Commission") for a Certificate of Public Convenience and Necessity ("CPCN") to provide full facilities-based and resold competitive local exchange access and non-dominant interexchange services.[1] On May 15 2017, ORA protested PG&E's Application identifying several issues including network resiliency and security; ORA cited PG&E's test year 2017 General Rate Case ("GRC"), where PG&E considered cyber-attacks as the utility's highest priority enterprise risk.[2] The Scoping Memo and Ruling of Assigned Commissioner and Administrative Law Judge ("Scoping Memo"), filed July 13 2017, recognized ORA's concerns as within the scope of the proceeding by asking "[d]oes this Application raise issues related to privacy, cybersecurity, or other subjects that should be addressed before a CPCN is granted? If so, what are those issues and how should they be addressed?"[3] This testimony examines PG&E's plans and existing telecommunications infrastructure to determine if granting PG&E a CPCN to operate as a Competitive Local Exchange Carrier ("CLEC") will increase its cybersecurity or safety risks and how those risks could be mitigated.

If PG&E's request for a CPCN is granted, the Commission should require and hold PG&E accountable to establish and maintain a physical and virtual separation of the PG&E's utility gas and electric telecommunications network ("Utility Network") and its proposed CLEC telecommunications network ("CLEC Network").[4] To maintain a physical and virtual network separation, PG&E **should not** co-mingle CLEC and utility gas and electric active network

[1] PG&E proposes to use excess capacity on its existing ratepayer funded telecommunications network to provide telecommunications services. Shareholders will fund any necessary extensions to PG&E's network needed to provide service to new customers.

[2] A.15-09-001, 2017 General Rate Case Prepared Testimony of PG&E on Shared Services and Information Technology, Chapter 10 at page 10-2. In response GRC-2017-Phl_DR_ORA_025-Q11Atch01 the Data Response of PG&E to ORA Data Request 25, Question 11 in A.15-09-001 PG&E provided a table illustrating how various risks rank within all risks that PG&E faces. In this response, Cybersecurity was rated the #11risk with a risk score of 586 beneath risks such as wildfire, catastrophic gas pipeline failure, and serious injury or fatality to employees or contractors.

[3] Scoping Memo at page 8

[4] In general, a telecommunications network is a collection of network equipment, transmission links, and control systems that are connected together to allow for the transmission and exchange of information among multiple users. Utility Network refers to the collection of network equipment, links, and controls used to support PG&E's utility gas and electric operations. CLEC Network refers to the collection of network equipment, links, and controls used to support PG&E's proposed CLEC telecommunications operations.

equipment,[5] control equipment, fiber strands. PG&E **should** separate Utility Network infrastructure data and customer data from CLEC Network infrastructure data and customer data. Furthermore, there should be no direct connection or indirect connection between PG&E's Utility Network and PG&E's proposed CLEC Network to ensure that a breach of one network does not compromise the other network.

[5] CLEC_DR_ORA_001-Q06 PG&E response to ORA DR No. 1, Question 6: Active network equipment is the equipment used to direct and terminate telecommunications service such as: switches and multiplexers

I. INTRODUCTION

In its September 22 2017 prepared testimony, PG&E described its business plans, telecommunications network, and network operations group. PG&E states that its Telecommunications Infrastructure and Operations ("I&O") group, a significant portion of PG&E's Information Technology ("IT") department, is responsible for the installation, monitoring, and maintenance of PG&E's telecommunications and network equipment throughout the service territory.[6] PG&E has a security organization that handles network and cybersecurity as a peer organization to the I&O group within PG&E's IT department.[7] The IT department operates a "24 x 365" Network Control Center that provides its clients a single point of contact for operational or maintenance issues. PG&E plans to use the same IT employees to support PG&E's existing networks and the proposed CLEC Networks and plans to mitigate increased cybersecurity risk to the Utility Network by establishing and maintaining physical and virtual separation of the Utility Network from the CLEC Network.[8]

As operations shift from manual processes to the Internet, electronic, and cloud based platforms, organizations need to evaluate and mitigate potential cybersecurity risks that will arise. Cybersecurity risk increases as more devices, connections, and users are added to a network. In recent years, bad actors and cyber criminals have taken advantage of businesses and government organizations' increasing reliance on connectivity and cybersecurity vulnerabilities to launch attacks, shut down operations, and extract sensitive information.[9]

Recently, hackers have begun targeting energy utilities; this is best represented by the December 23 2015 hack of the Prykarpattyaoblenergo electric utility in Ukraine. Hackers took nearly 30 substations offline across three distribution centers, disabling back up power to two of those distribution centers, disabled monitoring stations, overwhelmed the utility's customer service call centers, and left more than 230,000 residents without power in the winter months for

[6] The Prepared Testimony of PG&E Chapter 5 at page 5-1.
[7] CLEC_DR_ORA_001-Q09: PG&E's Response to ORA's Data Request No. 1, Question 9.
[8] The Prepared Testimony of PG&E Chapter 5 at page 5-3.
[9] For example: In December 2016 the San Francisco Municipal Transport Agency was subject to a Ransomware attack that compromised its transit systems. In 2013 Target suffered a cyberattack that leveraged a vulnerability involving a third party contractor to gather financial information from approximately 110 million customers. In May 2017, Equifax suffered a breach that compromised sensitive personal information on approximately 143 million Americans.

up to six hours.[10] The attackers also damaged critical devices at 16 of the affected substations, leaving the devices unresponsive to remote commands from operators. In May 2017, Cisco's Talos Intelligence group noticed an increase in spear phishing specifically targeting the energy sector, stating that "Talos has identified an email-based attack targeting the energy sector …"[11] On September 6, 2017 Symantec, a network security vendor, released a public statement regarding a group of hackers that are explicitly targeting the energy sector in Europe and North America. Symantec stated that "The energy sector in Europe and North America is being targeted by a new wave of cyber-attacks that could provide attackers with the means to severely disrupt affected operations."[12]

As cybercrime continues to evolve, proper cybersecurity protections become increasingly more important. Hackers are compromising vulnerable networks to steal sensitive customer information, disrupt operations, and ransom computer systems. The Federal Bureau of Investigation's ("FBI") Internet Crime Complaint Center ("IC3") received almost 300,000 complaints and tallied reported losses in excess of $1.3 billion in 2016.[13] Furthermore, the IC3 notes that total reported losses due to cybercrime have increased every year since 2012. The Commission must ensure that PG&E will not increase the cybersecurity risk to its gas and electric operations because of its proposed CLEC operations.

[10] WIRED News explores the unprecedented Hack of Ukraine's Power Grid: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
[11] Talos, Attacks on Critical Infrastructure Leverages Template Injection: https://blog.talosintelligence.com/2017/07/template-injection.html
[12] Dragonfly: Western energy sector targeted by sophisticated attack group: https://www.symantec.com/connect/blogs/dragonfly-western-energy-sector-targeted-sophisticated-attack-group
[13] The FBI's IC3 2016 Annual Report, Introduction: https://www.ic3.gov/media/annualreport/2016_IC3Report.pdf

II. SUMMARY OF RECOMMENDATIONS

PG&E should provide the Risk Assessment and Mitigation Phase ("RAMP") submission and risk register that is associated with cybersecurity, currently due to be filed by December 2017, in its rebuttal testimony. PG&E should provide a description of the difference in threats, risks, and ranking between their past risk submission in the 2017 GRC and the pending RAMP filing. In addition, PG&E should provide the metrics it will use to evaluate cybersecurity risk in its upcoming RAMP submission, as well as the metrics it used to evaluate cybersecurity risk in its most recent GRC.[14]

If PG&E's CPCN is granted, the Commission should not open up the electrical supply space to CLEC fiber attachments. The Commission should adopt the recommendations outlined below as conditions to the approval of PG&E's CPCN to keep PG&E's Utility Network and CLEC Network separate:

- Gas and electric data should be physically and virtually separate from CLEC customer data.
- CLEC customer data should be carried on different fiber strands, different network equipment, different control equipment, and different telecommunications networks than Utility gas and electric data.
- PG&E should not store Utility Network data, customer data, and energy infrastructure information in any databases that are shared with the CLEC Network or that are accessible through the CLEC Network.
- There should be no direct and no indirect connection between PG&E's utility gas and electric telecommunications network and PG&E's proposed CLEC telecommunications network so that a breach of one network does not compromise the other network.
- The Commission, ORA and the Office of the Safety Advocate ("OSA") should be notified of any breach with or involving the CLEC Network within 24 hours. PG&E should provide a report of what happened and how it plans to mitigate the breach in the future within 10 days.

[14] In A.15-09-001, PG&E filed September 1, 2015 testimony on Shared Services and Information Technology where the utility stated in Chapter 10, page 10-2 that "In fact, [cybersecurity] is PG&E's highest priority enterprise risk."

III. DISCUSSION

To determine if risk will increase, risk must first be quantified. Organizations and industries often develop a way to quantify the inherent risks of operations. International Business Machines ("IBM") suggested a formula that characterizes risk of cyber threats in the electric sector as: the Threat a cyber-attack occurring times the Vulnerability of utility grid systems times the Impact of a successful cyber-attack.[15] The Threat of cyber-attack increases as electric power systems interconnect to other networks and external hacking attempts grow more prolific. The Vulnerability of grid systems increases as highly connected networks offer new paths for hackers to attack critical operational systems. The Impact of a successful cyber-attack is severe because critical electrical systems operations are increasingly interconnected to other systems and controlled remotely.

Evaluating the potential danger of cyber-attacks faced by modern utility operations is salient as cyber-attacks no longer pose insignificant risk. Particularly, the Congressional Research Service ("CSR") reported over a decade ago, in 2004, that:

> *"Because of the greater degree of automation and computer control in electric utilities, the ability of an electric utility to provide and maintain electric service could be compromised by cyber-attacks that target industrial control systems or through a cyber-attack that significantly degrades the ability of these computerized systems to process commands and signals."*[16]

PG&E's proposed CLEC business will add more connections, devices, and users to the existing telecommunications infrastructure, and create more pathways and avenues for attack for hackers to exploit. The more pathways available for an attacker to use to orchestrate an attack on PG&E's networks, the more vulnerable PG&E's networks would be, increasing operational risk. It is important to examine how PG&E plans to mitigate the increased risk of operating a CLEC Network in parallel with a Utility Network.

---

[15] IBM's White Paper: Best practices for cyber security in the electric power sector ("IBM White Paper"), page 4. Risk = Threat x Vulnerability x Impact. The White Paper can be found here: https://www.ibm.com/services/multimedia/WR928534SF-Best_practices_for_cyber_security_in_the_electric_power_sector.pdf

[16] The Congressional Research Service April 2004 report on Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism, page 22. The Congressional Research Service serves as a public policy research agency for the United States Congress. The 2004 report can be found here: https://digital.library.unt.edu/ark:/67531/metadc807647/m2/1/high_res_d/R42795_2004Apr09.pdf

ORA based its analysis of PG&E's cybersecurity risk on standards and guidelines published by federal agencies and industry leaders such as the National Institute of Science and Technology ("NIST"), the Federal Financial Institutions Examination Council ("FFIEC"), the North American Electric Reliability Corporation ("NERC"), the CSR, and IBM. Existing standards cover a wide range of cybersecurity and network security management topics. NIST's Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") contains five high level fields called functions. These functions are: Identify, Protect, Detect, Respond, and Recover. Each function has categories and subcategories that define its specific technical needs and outcomes. As this testimony focuses primarily on how the vulnerability of PG&E's Utility Network is affected by the proposed CLEC business, the analysis will focus on the Protect function as defined in the Cybersecurity Framework to best characterize the steps PG&E is taking to mitigate the vulnerability of more connected network by controlling access to its Utility Network and clearly segmenting its Utility Network from its proposed CLEC Network. To protect electric and gas infrastructure and operations, the Commission must ensure that PG&E holds to the commitments it has made to keep its CLEC Network and Utility Network separate.

A. Network Security and Segmentation

One way PG&E can reduce its vulnerability to cyber-attacks is by limiting the avenues of attack on their critical systems. This approach improves cyber security on multiple fronts by making it easier to protect the Utility Network's perimeter, monitor for possible intrusion, and gives attackers less options for attempting attacks. More connections to the network, more devices on the network, and more parties able to access the network all increase vulnerability, which increases cybersecurity risk.[17] One way of reducing this vulnerability is to reduce the number of parties and devices with access to the network. Another option is to segregate critical networks from other networks, which can be accomplished by creating a private Wide Area Network ("WAN") or using a Virtual Private Network ("VPN") to keep critical network traffic secure. IBM recommends that utilities segment sensitive systems, data, and information stating that "…it still makes sense to eliminate unnecessary interconnectivity between sensitive data and

[17] The FFIEC Cybersecurity Assessment Tool illustrates this on Page 11, showing an increasing risk level as more types of devices connect to the network in greater number and as more third parties gain access to the system. The Tool can be found here: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

insecure networks…"[18] NIST's Cybersecurity Framework recommends these precautions in the access control category stating networks should be segregated where appropriate and that access to systems and network assets should be controlled.[19]

PG&E has acknowledged the importance of keeping the Utility Network and CLEC Network separate to ensure important systems are secure, stating that "PG&E will dedicate separate strands of fiber for CLEC customer traffic and use separate end-point equipment that will have no data, control, or communications connection to PG&E's utility telecommunications gear and secure spaces."[20] In the event that CLEC and utility gas and electric communications equipment are in the same rooms, PG&E stated that CLEC equipment will be clearly documented and labeled but did not provide an assessment of the risk or consequences of inadvertently connecting Utility Network equipment and CLEC Network equipment. PG&E then further elaborates, stating that "… any configuration changes or manipulations of the CLEC customer active network equipment will not impact gas and electric networks, data or active network equipment."[21] Furthermore, PG&E intends to keep operations data separate by displaying CLEC Network data on different network maps and tables than Utility Network data.[22] Network maps are generated from PG&E's network monitoring platform or created in computer aided design programs. These maps can be presented electronically or printed. PG&E currently plans to store certain Utility Network data and CLEC Network data in shared databases.[23] [24] Storing Utility Network data in a shared database that is accessible from the CLEC Network creates new pathways to access Utility data.

Storing Utility Network and CLEC Network data within shared databases could increase PG&E's cybersecurity risk. If sensitive Utility Network data, customer data, or critical energy infrastructure information ("CEII")[25] is collocated with CLEC data in a shared database and that

[18] IBM White Paper, Page 9: Recommended Action 3 "Segment sensitive systems and information."
[19] NIST's Cybersecurity Frame work, page 24, at PR.AC5 and Page 29 at PR.PT-3. NIST's Cybersecurity Framework can be found here: https://www.nist.gov/document-3766
[20] *Reply of Pacific Gas and Electric Company (U 39 E) To Protests* filed on May 25, 2017, page 9.
[21] CLEC_DR_ORA_001-Q01: PG&E's Response to ORA's Data Request No. 1, Question 1.
[22] CLEC_DR_ORA_001-Q13: PG&E's Response to ORA's Data Request No. 1, Question 13.
[23] CLEC_DR_ORA_003-Q03: PG&E's Response to ORA's Data Request No. 3, Question 3.
[24] Any information stored in a shared database will be encrypted to protect against unauthorized users gaining access to the information.
[25] The Federal Energy Regulatory Commission defines Critical Energy Infrastructure as a system or asset of the bulk-power system, (physical or virtual) where the incapacity of destruction of which would negatively affect: national security, economic security, public health or safety, or any combination of such matters.

data could be accessed from the CLEC Network it increases the possibility of CEII being compromised, as this creates a new pathway for hackers to use.[26] PG&E should not store Utility Network data, customer data, and critical energy infrastructure information in databases that are shared with the CLEC Network or accessible through the CLEC Network.

B. Network Operations

PG&E can also reduce cyber-risk by monitoring and controlling the devices on its networks. Good Cybersecurity practices include monitoring for possible intrusions and keeping awareness of the state of equipment and data traffic.[27] NIST's cybersecurity framework recommends defined configuration change protocols to prevent unauthorized changes and that an organization should check the integrity of its software and firmware. Rigorous logs, change management processes, and baseline configurations provide ways to detect if a device has been compromised or an intrusion has occurred. Organizations should also have a plan to respond to incidents after an intrusion or misconfiguration has been detected.

PG&E intends to use the same network monitoring platform and Enterprise Network Operating Center ("ENOC") to monitor both Utility and CLEC Networks.[28] The ENOC will act as a central operating point for both PG&E's Utility Network and CLEC Network. The network monitoring platform PG&E uses resides on PG&E owned equipment inside PG&E owned data centers. PG&E plans to monitor the CLEC Network using out-of-band equipment and a unique VPN.[29] Out-of-band monitoring uses data transferred through an out-of-band data stream that is independent from the in-band data stream and operates on a management plane that is separate from the data plane that is used by in-band data traffic. This separation means that out-of-band monitoring and management devices can function during periods of traffic congestion, equipment malfunction, or attacks on the network. Certain network elements like switches can be configured to prevent access to the out-of-band management port from the in-band data ports, preventing malicious attempts to access the management network from the data plane and improving overall network security.

[26] The 2017 Equifax breach was the direct result of vulnerability in the Apache Struts 2 web application framework that allowed malicious actors to bypass authorization and extract sensitive information from Equifax databases.
[27] IBM White Paper, Page 9: "Control your endpoints." And "Protect your networks."
[28] CLEC_DR_ORA_001-Q13: PG&E's Response to ORA's Data Request No. 1, Question 13.
[29] CLEC_DR_ORA_001-Q03: PG&E's Response to ORA's Data Request No. 1, Question 3.

In addition to out-of-band monitoring to keep track of the CLEC Network, PG&E maintains methods of procedure ("MOP") to dictate workflow and the process of changing the configuration of network equipment or elements. The MOP contains step by step instructions to obtain authorization and carry out requests, including timelines for review and approval. In some instances, the MOP contains individual procedures that have step by step instructions for a technician to carry out.[30] The MOP has a workflow process for obtaining emergency approval of configuration changes in the event of critical equipment is down or malfunctioning. If a misconfiguration or system outage occurs, PG&E will restore utility gas and electric traffic and services before third-party traffic and services.

C. PG&E's Business Plan

Risk assessment is a complex process that involves not just identifying and mitigating potential risks, but also defining acceptable levels of operational risk. Generally, organizations can reach an acceptable level of risk by implementing mitigation measures to reduce the impact of a particular risk or by addressing vulnerabilities in its systems. Sometimes an organization's leadership determines that the cost to reduce the impact or fix with vulnerabilities associated with a certain risk is too steep and mitigation measures are not implemented. In this instance, the organization chooses to accept a higher level of operational risk than initially planned.

PG&E's current plans and commitments to operate the Utility Network and the CLEC Network on separate fiber strands, end-point equipment, and networks not substantially increase the cybersecurity risk to PG&E's Utility Network. However, if PG&E changes its plans and connects the CLEC Network and Utility Network, PG&E's vulnerability to a cyber-attack increases and subsequently risk to PG&E's Utility Network increases. PG&E states that it is "evaluating a possible entry into the market as a… (CLEC) by looking at the significant assets available… which creates an opportunity to provide benefits to PG&E's ratepayers and shareholders"[31] and that "…changes in the communications industry may cause a situation where future objective evaluation shows that continuing to offer CLEC services no longer makes business sense."[32] PG&E plans to use a gated approach that allows it to "…suspend the process

[30] CLEC_DR_ORA_001-Q14Atch01
[31] Prepared Testimony of PG&E Chapter 2 at page 2-4
[32] *Id.*

at various points in the approval and implementation process in order to reassess the risks and benefits of the proposed business."[33]

PG&E's CLEC business will be undergoing continual assessment and PG&E has stated that it intends to take a cautious, gated approach in order to reassess risks and benefits as PG&E begins its CLEC business. If part of reassessing the risks involved in PG&E's CLEC business includes increasing the level of acceptable cybersecurity or safety risk to lower the cost or challenge of implementing CLEC operations, PG&E's Utility Networks would be put at increased risk as a result. The Commission should adopt clear requirements to keep PG&E's Utility Network and CLEC Network physically and virtually separate, consistent with current PG&E commitments outlined above, to ensure the security, safety and reliability of PG&E's Utility Network and California gas and electric infrastructure and operations.

D. Fiber Cable in the Electrical Supply Space

PG&E stated that some of its existing fiber cables are installed in the electric supply space on distribution poles.[34] The Commission should adopt the recommendations made in Mr. Clark's testimony concerning fiber in the electric supply space.

Allowing PG&E or any other CLECs to install fiber in the electrical supply space raises significant safety concerns. It would be unsafe to allow workers that are potentially unfamiliar with electrical distribution equipment into the electric supply space to string fiber. The safety of the worker, the electric distribution equipment, and the public would be put at risk. PG&E stated that fiber in the electric supply space is difficult to maintain and repair due to issues gaining access to the infrastructure.[35] It would be unwise to compound that difficulty by allowing PG&E or any other company the ability to string fiber in the electric supply space. Furthermore, in recent years several brush fires were caused by broken lashing wire that came off communications lines and caused electrical arcing.[36] The risk of power line damage is increased

[33] *Id.*
[34] Prepared Testimony of PG&E Chapter 2 at page 2-2
[35] *Id*
[36] California Department of Forestry and Fire Protection ("CalFire") report on the Guejito Fire, "the fire was determined to have started when energized power lines and lashing wire from a Cox Communications cable came in contact with each other." The report summary can be found here: http://calfire.ca.gov/fire_protection/downloads/redsheet/CA_MVU_010484_Summary.pdf

if communications lines are installed directly in the electrical supply space. The Commission should not open up the electrical supply space to CLEC fiber attachments.

IV. CONCLUSION

In order to mitigate the potential risks of operating a CLEC network in parallel with a utility gas and electric telecommunications network, PG&E should not co-mingle CLEC and Utility active network equipment, customer data, control equipment, or fiber strands and should keep its Utility Network and CLEC Network physically and virtually separate. Furthermore, there should be no direct or indirect connection between PG&E's Utility Network and PG&E's proposed CLEC Network so that a breach of one network does not compromise the other network. PG&E should not store Utility Network data, customer data, and critical energy infrastructure information in databases that are shared with the CLEC Network or accessible through the CLEC Network. PG&E should inform the Commission of any new risks or change in cybersecurity it expects as a result of operating a CLEC business in its upcoming RAMP submission.

The Commission should ensure that PG&E follows through its stated commitment to keep the CLEC data and equipment and Utility data and equipment separate by adopting the above recommendations as conditions for approving the CPCN application.

ATTACHMENTS

ATTACHMENT A

Statement of Qualifications and Experience

My name is Cameron Reed. I am currently employed by the California Public Utilities Commission ("Commission") as a Utilities Engineer assigned to the Communications and Water Policy Branch of the Office of Ratepayer Advocates ("ORA"). I have a Bachelor of Science in Mechanical Engineering from the University of California, Davis. My studies included courses in engineering control systems, electric circuits, experimental methodology, and mechanical systems design. While at Davis I completed several projects including designing a measurement rig that would analyze the force and energy distribution present in the grinding process. I am a member of the Phi Theta Kappa honor society.

I joined ORA in July 2016. I have worked on evaluating California Advanced Services Fund ("CASF") Infrastructure and Public Broadband Housing applications. The CASF program funds broadband deployment in unserved or underserved areas of California and involves evaluating company financial information, deployment plans, and any existing broadband infrastructure in the project area. I have participated in Application ("A.") 16-10-003, the General Rate Case of Sierra Telephone Company, submitting testimony evaluating the company's Public Safety and 9-1-1 Network. I also participated in A.17-03-016, the Acquisition of Level 3 Communications by CenturyLink where I reviewed issues such as: service outages, network infrastructure, and fiber redundancy. I am currently participating in Rulemaking 17-03-009 and 17-06-028 and Investigation 17-06-027 regarding access to poles and a centralized pole database. In the course of monitoring telecommunications service quality and safety, I have reviewed hundreds of Federal Communications Commission Network Outage Reporting System outage reports. I am generally familiar with the current discussion regarding Grid Modernization and have assisted in the review of Southern California Edison's ("SCE") Grid Modernization proposal during SCE's A.16-09-001 General Rate Case.

During my time at the Commission, I have completed the National Exchange Carrier Association's Foundations of Telecommunications Curriculum and the National Association of Regulatory Utility Commissioner's Utility Rate School.

Docket:	A.17-04-010
ORA Expert Witness:	Cameron Reed
Date:	November 22, 2017

Office of Ratepayer Advocates

Attachment B

PG&E Response to ORA Data Request No. 1

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q01		
PG&E File Name:	CLEC_DR_ORA_001-Q01		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 1

Please describe all security measures, such as separate user accounts or different passwords for Network Equipment, which PG&E intends to use to keep its existing telecommunications and corporate networks secure and separate so that a breach in CLEC Operations will not compromise Utility Operations.

ANSWER 1

The CLEC customer network will utilize different active network equipment than the active network equipment carrying Utility gas and electric networks and data. Active network equipment comprises the components used to transmit signals. Therefore, any configuration changes or manipulations of the CLEC customer active network equipment will not impact gas and electric networks, data or active network equipment.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q02		
PG&E File Name:	CLEC_DR_ORA_001-Q02		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 2

In *Reply of Pacific Gas and Electric Company (U 39 E) To Protests* filed on May 25, 2017, PG&E states on page 9 that, "…CLEC customer traffic… will have no data, control, or communication connection to PG&E's utility telecommunications gear and secure spaces." Does this mean there will be no direct connection between telecommunications gear and secure spaces such that no one piece of CLEC network equipment is linked to Utility network equipment by a single cable or shared computer? Please explain what types of connections (i.e. direct or indirect) that will exist between PG&E's utility telecommunications network equipment and the CLEC telecommunications network equipment.

ANSWER 2

There will be no data connection, either direct or indirect, between CLEC network active equipment and Utility gas and electric network active equipment.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q03		
PG&E File Name:	CLEC_DR_ORA_001-Q03		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 3

In *Reply of Pacific Gas and Electric Company (U 39 E) To Protests* filed on May 25, 2017, PG&E states on page 9 that, "…CLEC customer traffic… will have no data, control, or communication connection to PG&E's utility telecommunications gear and secure spaces." Does this mean that PG&E will have separate Network Operations Centers for Utility Operations and CLEC Operations? If no, please describe how PG&E intends to separate Network Operations Centers for Utility Operations from CLEC Operations.

ANSWER 3

The PG&E Enterprise Network Operations Center (ENOC) will monitor both Utility and CLEC networks. The Utility and CLEC networks will not be directly connected to each other. Current plans involve utilizing out of band equipment via a unique VPN to monitor CLEC telecom equipment.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q04		
PG&E File Name:	CLEC_DR_ORA_001-Q04		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 4

If the Utility and CLEC Operation Centers are separate, would the Utility and CLEC Operation Centers be indirectly connected through a PG&E wide area network, field area network, or other corporate network, to either a centralized Network Operations Center or other Operations Centers?

ANSWER 4

Please refer to Answer #3

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q05		
PG&E File Name:	CLEC_DR_ORA_001-Q05		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 5

In *Reply of Pacific Gas and Electric Company (U 39 E) To Protests* filed on May 25, 2017, PG&E states on page 9 that, "…PG&E will dedicate separate strands of fiber for CLEC customer traffic and use separate end-point equipment..." Will the end-point equipment for Utility Operations and CLEC Operations be co-located within the same PG&E secure rooms or equipment racks? If so, will the end-point equipment for each network be clearly indicated as belonging to separate networks?

ANSWER 5

In certain circumstances, CLEC network active equipment may be located in the same secure room as Utility network active equipment. CLEC network equipment will be documented and clearly labeled as CLEC network equipment.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q06		
PG&E File Name:	CLEC_DR_ORA_001-Q06		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 6

In *Reply of Pacific Gas and Electric Company (U 39 E) To Protests* filed on May 25, 2017, PG&E states on page 9 that, "…PG&E will dedicate separate strands of fiber for CLEC customer traffic and use separate end-point equipment..." Please describe what equipment PG&E defines as end-point equipment.

ANSWER 6

In this context, end point equipment is defined as active equipment used to terminate services to a CLEC customer at the customer's premises. Examples of this type of equipment would be but not limited to: routers, switches, SONET network elements, and DWDM equipment.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q07		
PG&E File Name:	CLEC_DR_ORA_001-Q07		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 7

Is PG&E's existing telecommunications network connected to Internet Exchange Points? If not, does PG&E intend or expect to connect its existing telecommunications network to any Internet Exchange Points as a result of the CLEC business?

ANSWER 7

The PG&E Utility network is currently connected to Internet Exchange Points.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q08		
PG&E File Name:	CLEC_DR_ORA_001-Q08		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 8

On page 2-AtchA-1, in the third table entry for the 2014 GRC for chapter 8 page 33 lines 1-9 of the *Prepared Testimony of Pacific Gas and Electric Company* filed September 22, 2017, PG&E mentions "PG&E's common facilities (i.e., communication rooms, mountain tops, communication buildings, antenna towers, generators, cable plants, high-voltage protection and battery plants) …" What PG&E common facilities will be shared between PG&E's Utility network and the proposed CLEC's network?

ANSWER 8

In certain circumstances, CLEC telecom network active equipment may be located in the same secure room as Utility network active equipment. In these cases CLEC network active equipment and Utility network active equipment would typically share the communications room, generator, DC plant, telecom alarm remote terminal unit, and HVAC.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q09		
PG&E File Name:	CLEC_DR_ORA_001-Q09		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 9

On page 5-1 of the *Prepared Testimony of Pacific Gas and Electric Company* filed September 22, 2017, PG&E states that, "[t]he I&O group is responsible for the installation, monitoring, and maintenance of PG&E telecommunications and network equipment throughout the service territory." Is the I&O group also responsible for telecommunications network security? If no, who is responsible for telecommunications network security?

ANSWER 9

The Security organization which encompasses Network and Cyber Security is a peer organization to the I&O organization in PG&E's IT department.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q09		
PG&E File Name:	CLEC_DR_ORA_001-Q10		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 10

Will the group identified in the response to Question 9 be responsible for network security and management on both PG&E's CLEC network and Utility network?

ANSWER 10

The Security organization which encompasses Network and Cyber Security is responsible for network security on the Utility gas and electric network. PG&E currently plans to address responsibilities for CLEC customer network security on a contractual basis.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q11		
PG&E File Name:	CLEC_DR_ORA_001-Q11		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 11

On page 5-1 of the *Prepared Testimony of Pacific Gas and Electric Company* filed September 22, 2017, PG&E states that, "[t]he I&O group is responsible for the installation, monitoring, and maintenance of PG&E telecommunications and network equipment throughout the service territory." Please explain what metrics and methods, such as network traffic or alarms, the I&O group uses to monitor PG&E's telecommunications network.

ANSWER 11

PG&E's Enterprise Network Operations Center (ENOC) operates as the central nerve center for IT, providing customer focused, best in class service. With its skilled, multi-tiered workforce, ENOC supports network management, incident and problem management, change management, technical support, business rule management, and network monitoring and scheduling. ENOC utilizes a suite of network management tools to monitor, evaluate, and troubleshoot the network. These tools include high level alarm monitoring tools as well as tools for analysis of traffic flows and link utilization.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q12		
PG&E File Name:	CLEC_DR_ORA_001-Q12		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 12

On page 5-2 of the *Prepared Testimony of Pacific Gas and Electric Company* filed September 22, 2017, PG&E states that "IT also has a "24x365" Enterprise Network Control Center that provides a single point of contact for any operations and maintenance issues the clients of the IT organization may have." Will the Enterprise Network Control Center support or otherwise monitor, manage, or control both Utility Operations and CLEC Operations?

ANSWER 12

Please refer to Answer #3

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q13		
PG&E File Name:	CLEC_DR_ORA_001-Q13		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 13

Will any single systems (computers, Network Equipment, servers, etc.) within the Enterprise Network Control Center be directly or indirectly connected to both PG&E's Utility network and CLEC network? If so, what procedures does PG&E have in place, or plan to implement, to keep any identified systems secure?

ANSWER 13

It is planned that the PG&E Enterprise Network Operations Center (ENOC) will utilize the same network monitoring platform that is currently being utilized to monitor the Utility gas and electric networks. Connectivity to the CLEC network will be via a unique VPN. The CLEC telecom network will appear on different screens, network maps, and tables than the Utility gas and electric networks.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q14		
PG&E File Name:	CLEC_DR_ORA_001-Q14		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 14

On page 5-2 of the *Prepared Testimony of Pacific Gas and Electric Company* filed September 22, 2017, PG&E states that "A rigorous change management process is in place, which includes the incorporation of methods of procedure (MOP)…to ensure proper client notification and minimize the possibilities of mis-configuration." Please explain and provide a copy of these methods of procedure.

ANSWER 14

No work shall be performed on network equipment without first filing a Request for Change (RFC). As part of the RFC, a Method of Procedure (MOP) must be included. The RFC and MOP are reviewed prior to approval and proper notifications are made to those who will be impacted by the RFC. Please see the two Attachments CLEC_DR_ORA_001-Q14Atch01 and CLEC_DR_ORA_001-Q14Atch02 (including an excerpt from a sample MOP).

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q15		
PG&E File Name:	CLEC_DR_ORA_001-Q15		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 15

On page 5-4 of the *Prepared Testimony of Pacific Gas and Electric Company* filed September 22, 2017, PG&E states that "A rigorous change management process is in place which includes incorporation of the MOPs to ensure telecom equipment is properly configured." What does PG&E mean by properly configured? Do the MOPs include procedures for properly configuring network security measures?

ANSWER 15

Properly configured means that the needed modification to the network equipment is implemented as designed and no unintended impact to the equipment or the network occurs. PG&E has MOPs that describe the proper configuration of network security measures.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_001-Q16		
PG&E File Name:	CLEC_DR_ORA_001-Q16		
Request Date:	September 29, 2017	Requester DR No.:	001
Date Sent:	October 13, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Cameron Reed

QUESTION 16

Please identify all third party network security or end point protection providers that PG&E currently contracts with, or intends to contract with in the future.

ANSWER 16

PG&E objects to the scope of this data request. Specific information about PG&E's security controls implementation and the identities of the security vendors PG&E works with to protect our data and systems from advanced threat actors is highly sensitive, proprietary PG&E information. Disclosing this information would pose a threat to the security of the PG&E system. PG&E is able to share that PG&E uses security controls that are in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework and partners with the leading vendors and security service providers to ensure that PG&E data and systems are adequately protected.

Docket:	A.17-04-010
ORA Expert Witness:	Cameron Reed
Date:	November 22, 2017

Office of Ratepayer Advocates

Attachment C

PG&E Response to ORA Data Request No. 1, Question 14, Attachment 1

STANDARD OPERATING PROCEDURES

Standard Change:	Update shut/no shut change

Purpose:
The purpose of this change is to quickly do a shut/no shut on a switch port in case of error-disabled state. To perform this change requires that the Network Specialist to inform Network Operations Leadership for the device where the change will be performed.

Scope:
The scope of this request is for data network devices which include routers, physical & virtual switches. This change can be ran on all Network environments, UDN, ODN and GDN.

References:
Whenever there is a need to perform shut/no shut under specific interface on Routers, physical & virtual switches.

Who Can Perform Change:
A Network Specialist who is a member of one of the System Network Operations teams or the Solutions Build teams.

Frequency:

☒	Daily	☐	Weekly	☐	Quarterly
☐	Annually	☐	Other:		

Time Change Can Occur:

☒	Any time	☐	Core Business Hours	☐	After Hours only
☐	Weekend only	☐	Specific Day/Time:		

Procedures (Instructions):

Step	Description
1	Call ENOC and report on to begin Change
2	Confirm with ENOC there are no existing alarms on the equipment where the change will be made
3	Access network switch via approved terminal software Enable logging of your session, in case any issues arise.
4	Review current switch port configuration settings to ensure they align with what you are changing. (use the show interface command to ensure the port is truly err-disabled)
5	Enter enable mode if you are not already there
6	Config term
7	interface fastethernet slot/port (example)
8	shut
9	No shut
10	end
11	Writ mem
12	exit
13	Run a show interface fastethernet slot/port (example) to verify the interface is no longer err-disabled
14	If the server connecting to the port still have connectivity issues check with server admin and ask him to reboot the server and make sure the server negotiates right.
15	Upon configuration/server verification attach the session logs to the Standard CRQ
16	Call ENOC and Log off the CRQ.

Back out Plan:

Step	Description
1	As this change involves shutting down the port and bringing it back up with " no shut" we need to make sure that the interface comes backup " sh int status " and " "sh ip int bri " are used to verify.
2	interface fast Ethernet slot/port (example) no shut
3	end
4	Writ mem
5	exit

Impact:

Step	Description
1	There might be a momentary outage during the shut/no shut or server load which should be properly communicated to Server admin and ENOC.

Docket:	A.17-04-010
ORA Expert Witness:	Cameron Reed
Date:	November 22, 2017

Office of Ratepayer Advocates

Attachment D

PG&E Response to ORA Data Request No. 1, Question 14, Attachment 2

Telecom & Network Clearance/Change Request Procedure (G2002)

Summary

This document provides the procedures required to effectively and securely manage changes within the Network Infrastructure to ensure that changes to any information asset that can affect business applications, programs, systems software, hardware, or any other aspect of IT are applied in a controlled manner so that the stability and security of PG&E services are not compromised.

Before any new equipment is installed or existing equipment modified or removed from the PG&E Telecommunication and Data Networks, a Clearance/ Change Request (CRQ) must be scheduled by submitting a Telecommunication Service Request online form to ENOC Escalation and Clearance who approve and coordinate the Clearance/CRQ. The form identifies who, when, where, why, date, time, accounting, record of change and provides timeframes, objectives and directions from the requester to the ENOC Escalation and Clearance.

Clearances trigger Telecom Circuit Database activities, alarm monitoring changes, NERC CIP compliance and drafting updates. A Clearance/CRQ is needed so that affected groups can coordinate activities, down time can be arranged, notifications can be sent out and depending on the type of work associated with the change request, ensure that any related work is performed and that systems are brought back up upon completion of work.

A Clearance/CRQ is **required** for all network additions, modifications or removals. Work that is not considered a change or impact to the existing networks and systems can be conducted without a formal Clearance/CRQ.

Specialized Clearances/CRQs may require unique procedures depending on the impact to users, time of Clearance/CRQ, impact on business processes, and other variables.

Level of Use: Reference Use

Target Audience

Specialists

Telecom Technicians and Supervisors

Telecom Circuit Database personnel

ENOC Personnel

Network Services Specialists and Supervisors

Project Managers

Telecom & Network Clearance/Change Request Procedure (G2002)

Safety

Our systems carry traffic that is critical to the operational needs of PG&E, the State of California, and in some instances, the Western United States. Much of this traffic has a direct and real impact on the safety of our employees and the public at large. It is of critical importance that we do not introduce any situation that will result in interruptions.

The following safety guidelines should be followed when considering or implementing changes:

- Always perform a pre-task safety assessment of the planned work activities to ensure proper resources have been assembled.
- IT personnel must coordinate their work with the appropriate departments, must be trained as appropriate, and must be accompanied by a qualified worker, if needed.
- Contractors must always be accompanied by a qualified PG&E employee while working inside PG&E facilities.
- Always follow USP22 and the Code of Safe Practices.

Before You Start

If you are a Network Specialist or Telecom Technician you will enter the Clearance/CRQ in SMC so make sure you have access to the SMC Service Request Management module.

For new clients needing the SMC Service Request Management access:

- Call the TSC @ 8-223-9000.
- Install the BMC SMC software.

Every Clearance/CRQ has a lead time associated with it so make sure you allow for this when planning your work.

- Any Clearance/CRQ that impacts electric protection circuits requires **17 business days** minimum lead time for System Protection Review and ISO approval.
- All others require **10 business days** lead time.

Although emergency repairs do not require submitting a formal Clearance/Change Request/CRQ, these types of changes are the exception, not the rule. See **section 6. Emergency Repairs** for details about emergency repairs and procedures for getting the go-ahead.

Telecom & Network Clearance/Change Request Procedure (G2002)

Table of Contents

Subsection **Page**

Change Request Dependencies 3
Lead Time Requirements 5
Submitting the Change Request 5
Searching for Service Requests Awaiting Approval 5
Processing a Clearance/CRQ 6
Beginning and Completing the Work 8
Release Management High Level 9
Canceling or Extending a Clearance 9
Emergency Repairs 10
Appendix 1. Change Process Workflow 14
Appendix 2. Urgent, Energency Request Workflow 15
Appendix 3. Release Management Process Flow 16
Appendix 4. Example Telecom CHANGE Request Form 17
Appendix 5. Telecom Clearance Form Field Descriptions 18
Appendix 5. Telecom Clearance Form Field Descriptions 19
Appendix 6. Telecom Request for Approval Email 20
Appendix 7. Telecom Request for Approval Email 21

1. Change Request Dependencies

1.1. Any work that involves or affects Networkinfrastructure inside of a Data Center (FFIOC, RCIOC, and SFIOC) must be represented by the Requestor or Implementer at ECAB prior to the approval of the CRQ by ENOC.

1.2. Network Changes must indicate the network involved with the change being performed (ODN, UDN, GDN) and the location (FFIOC, SFIOC, RCIOC etc).

1.3. Changes involving Data Centers changes must be scheduled after business hours unless exemption is granted by ECAB.

1.4. Any work that has a high risk of affecting UDN or the phone system at a staffed location must be scheduled after business hours unless local coordination has been made in advance by the Requester and this is stated in the Clearance/CRQ scope of work description.

Telecom & Network Clearance/Change Request Procedure (G2002)

1.5. A request that involves a planned outage must include a Backout Plan. For Clearance purposes, an Outage is any service affecting work on IT Telecom/Network infrastructure, not necessarily the inability of PG&E to provide energy to its external customers.

1.6. A request that involves an outage of a SCADA Master Radio DAR circuit must include a corresponding list of impacted sites and device , which the Requester can obtain from the local SCADA Specialist.

1.7. A request that involves a Telecom infrastructure must include a list of impacted circuits/links/paths.

1.8. Hostnames for all network devices (routers, switches, voice gateways, servers, etc.) involved in the Clearance must be included in the description of work.

1.9. The Requester or their Supervisor notifies others affected by the Clearance/CRQ (for example, T200 Supervisor, and Specialist) and coordinates resources as needed.

1.10. The Requester submits the Clearance Request by creating a Service Request in SMC.

1.11. You may use the link below to directly go to the online Service Request Change Form:

https://smcweba.comp.pge.com/midtier/forms/itilappprdvip.comp.pge.com/SRS:ServiceRequestConsole/?mode=submit&F303900000=4&F303900900=SR005056A42DD8YCrEUAScbHMwzhrK&F303906700=0&F303902000=0&F303902100=0

NOTE

Clearance Requests must be reviewed and approved by a Supervisor, or Peer if submitted by a Network Specialist.

1.12. The Supervisor/Peer reviews the following information for the change to confirm that:

1. The request is accurate and a MOP is included
2. There is enough lead time for change type
3. Date/time does not adversely affect systems/clients
4. All information related to the change is included
5. Risk and impact has been assessed
6. Accounting (order numbers) are valid and will remain open until the work is completed
7. Systems affected are identified
8. Clients affected are identified
9. A back out plan is provided
10. SMEs, if needed, are included
11. ECAB Review is indicated if necessary
12. Additional approvals, if needed, are obtained (End User Approvals)

13. Email notification lists are included for notifications other than standard ENOC notifications

2. Lead Time Requirements

2.1. The requester must provide sufficient lead time for a Clearance to be analyzed by the ENOC followed by review and approval from appropriate stakeholders. The lead times below do not include the amount of time taken for Supervisor/Peer approval of the Service Request.

2.2. A minimum of 17 business/working days lead time is required for a Clearance/CRQ that will impact electric protection circuits due to LOB and ISO clearance processing requirements.

2.3. The lead time for a Clearance/CRQ that will impact Distribution can vary depending on available dates in the DO's calendar. Some dates may already be closed due to DO business requirements or resource constraints. See the link here for accessing the Application for Work (AFW). http://eo/afw/AFW1.asp

2.4. All other Clearances/CRQs require at least 10 business/working days lead time. A request that does not have sufficient lead time will be rejected and the Requester must provide a new schedule date.

3. Submitting the Change Request

3.1. The Network Specialist or the Telecom Technician submits requests directly in SMC as a Service Request. The Bolded fields on the form are required fields.

3.2. See Appendix 5. Telecom Clearance Form Field Descriptions, for the field descriptions.

3.3. A "pending approval" email goes to the owner of the LANID in the Supervisor field of the Service Request. The Telecom Supervisor or Network peer reviewer has 24 hours to review and approve the request. If the request is not approved in 24 hours, a notification is sent to the ENOC who is authorized to override the Approval for the Telecom Line Supervisor. The ENOC will NOT override for the Network peer reviewer. The Requester cannot revise a request after it has been submitted. If revisions are needed, the Requester should contact the Approver and the ENOC to change to details of the submitted change.

3.4. See the work guide here for for completeing a Service Request that will become a CRQ. http://wss/ovpio/sites/ENOC/eog1/Run%20Books/Change%20Management/Change%20Management%20Create%20a%20Change%20Request%20for%20Telecom%20and%20Networking%20Services.docx

3.5. After a CRQ is created, any modifications or updates to the CRQ should only be entered by ENOC, never by the Requester. If the Requester needs to modify content or fields in the CRQ, the Requester should send an email to ENOC for these changes to be made.

4. Searching for Service Requests Awaiting Approval

4.1. Beings the requests for change are submitted as service requests in the service request module, in order to locate the document after submission but before it has converted to a Change request CRQ you must search for it in the Service Request Web View.

4.2. To review requests that have been submitted but not yet approved, go to the Service Request module. Go to the Status field and select Waiting Approval from the drop down and click Search. Pre-CRQ Requests. Go to the Status field and select Waiting Approval. Click Search. This displays the queue of all service requests that have yet to be reviewed by a peer or processed.

4.3. See the work guide here for searching for a Service Request with the Requesdt Number: http://wss/ovpio/sites/ENOC/eog1/Run%20Books/Change%20Management/Change%20Management%20Search%20with%20Change%20Service%20Request%20number.docx

4.4. See the work guide here for searching for a Service Request without the Requesdt Number: http://wss/ovpio/sites/ENOC/eog1/Run%20Books/Change%20Management/Change%20Management%20Search%20without%20Change%20Service%20Request%20number.docx

5. Processing a Clearance/CRQ

5.1. See Appendix 1. Change Process WorkFlow

5.2. See the link here for general instructions on processing a general TNS (Telecom Network Services)CRQ: http://wss/ovpio/sites/ENOC/iemanagement/Procedures/Change%20Management/Change%20Management%20Processing%20a%20Change%20Request%20(CRQ)%20for%20the%20Utility%20Data%20Network%20(UDN).docx

5.3. After receiving the SMC Clearance Request or CRQ, ENOC Escalation and Clearance reviews the Clearance/CRQ for completeness (dates, times, lead time, accounting number, impact statements, backout plans, device names, verifies circuit numbers, identifies affected “downstream” links/circuits etc.).

5.4. Incomplete Clearances/CRQ’s will be returned to the requester for clarification/completion.

5.5. The circuits and routers are reviewed/processed through the Telecom Circuit Database for dependencies and Approvals and notifications required. After the circuit List is proiduced the raw data will give “most” of the Approvals that are required, but this should not be considered the complete list until all the circuits/functions are reviewed.

5.6. See the work guide here fopr processing a TCD Request through TCD: http://wss/ovpio/sites/ENOC/ecmanagement/Level%204%20Procedures/Change%20Management/Change_Management_How_to_Process_a_Circuit_List_in_Telecom_Circuit_Database_(TCD).docx

5.7. CRQ and circuit data will be then reviewed for the following additional processing to include but not limited to:

1. **Electric Protection** – Work that will impact electric protection circuits will require submission for System Protection review and cutout instructions. This additional processing will require additional processing time required by the System Protection

Engineering staff. System Protection review followed by TOCOC and CAISO review and approvals will take a minimum of 17 days lead time. See the work guide here for processing Electric Protection CRQ: http://wss/ovpio/sites/ENOC/ecmanagement/Level%204%20Procedures/Change%20Management/Change%20Management%20Processing%20Electric%20Protection%20Change%20Requests%20(CRQs).docx

2. **Distribution Operations** – If there is an outage indicated on the CRQ, and it involves Distribution Operations circuits, the CRQ lead time may be driven by the impacted DO calendar(s). This CRQ will then need to be processed through the impacted DOs via an Application for Work (AFW).

3. See the work guide located here for instructions on processing an Application for Work: http://wss/ovpio/sites/ENOC/ecmanagement/Level%204%20Procedures/Change%20Management/Change_Management_Processing_a_Telecom_Clearance_with_Distribution_Operations_Involvement.docx

4. **TOCOC/ CAISO Review** – If the CRQ involves Electric ODN, Transmission circuits, the CRQ will require review by at least TOCOC and could require CAISO (California Independent System Operator) review. This will require10 business days lead time.

5. **Fiber** – If there is an outage indicated on the CRQ and the circuits include Fiber cables/links/rings/etc., the CRQ may require additional processing time to be reviewed by a fiber specialist or Telecom Transport SME at the discretion of the ENOC.

6. **ECAB** –Changes that meet at least one of the criteria below, the change ticket must be flagged for review by the E-IT CAB.

    - Change impacts any Tier 1 system or facility or Tier 2 system
    - Change impacts 500 or more users
    - Change involves high risk of failure or high impact to business
    - Involves Data Center network infrastructure

    Changes to be reviewed by the E-IT CAB must be scheduled 14 days in advance of the requested change date. The E-IT ECAB meets weekly to review all scheduled changes.
    ECab Review is tracked in the Approvals Tab of the CRQ.

    CRQ that requires ECab approval must be moved to “Work in Progress” before an ECab review and approval will occur. A clearance/CRQ that requires ECab review must be placed in the status of “Work in Progress” to e reviewed in the meeting.For more information on ECAB please use the following link: http://pgeweb/topics/ITSM/Pages/Enterprise%20IT%20CAB.aspx

5.8 The ENOC submits the Change Request/Clearance/CRQ to other approvers, as needed to the following groups:

- DCPP (Diablo Canyon Power Plant)

- DOs (Distribution Operations) via Application for Work
- Enterprise Storage (Replication Tape)
- Gas Control (Gas Operations)
- Hydro (EPOS) Energy Procurement Operations
- Network Operations
- System Protection Engineering
- RMC (Resource Management Center)
- SmartMeter
- TOCOC (Transmission Operations Center Outage Coordination)
- Work Force Management (WFM) (Contact Centers)

After receiving all required approvals, ENOC Escalation and Clearance issues an approval notification via email to the requester and stakeholders.

NOTES

The requester will be responsible for obtaining approvals from any groups or individuals not listed above. The ENOC Escalation and Clearance is not authorized to send notifications to PG&E Outlook distribution lists representing site end-users, nor to Outside Agencies. The requester should only begin the work once an approval notification is received. The requester should not assume that a submitted Clearance/CRQ is automatically approved and is responsible for checking on the status.

6. Beginning and Completing the Work

6.1. Prior to beginning work, the requester “signs on” by calling ENOC Escalation and Clearance at 1-800-892-9743, 1-415-973-3662, or co. 223-3662.

See the work detail here for checking in and out of a clearance with the ENOC. http://wss/ovpio/sites/ENOC/ecmanagement/Level%204%20Procedures/Change%20Management/Change%20Management%20Checking%20Change%20Requests%20(CRQs)%20In%20and%20Out.docx

7. Release Management High Level

See Appendix 3. Release Management Process Flow

7.1. The ENOC logs the check in call in a CRQ Work Detail.

7.2. The ENOC contacts appropriate LOB or outside agency for final OK to proceed.

7.3. The ENOC and validates all alarms are cleared and any cutouts have been made.

7.4. The ENOC gives the go-ahead to the requester to proceed with the work.

7.5. Upon completing the work, the requester "signs off" by calling the ENOC.

7.6. The ENOC verifies that all services are restored upon work completion.

7.7. The ENOC confirms the work is complete and "releases" the tech.

7.8. The ENOC completes the SMC tag detailing the work and changes the status to **Complete** to close out the request.

Notes

The tech responsible for updating the TCD contacts the TCD team to make sure changes are made. The source documentation for the change, which is usually provided to the Com Tech by the Telecom Engineer, must be provided to the TCD team and it should show the circuit path that will result after the change has been implemented. Refer to the Telecom Circuit Database (TCD) Information Guide for more details.

8. Canceling or Extending a Clearance

8.1 To extend a Deployment in Progress Clearance/CRQ by more than 24 hours past its approved End Date/Time, the requester should call ENOC Escalation and Clearance, who may either grant the extension directly or instruct the requester to obtain approval for rescheduling.

8.2 To cancel a Clearance/CRQ before its scheduled date and time, notify the ENOC Escalation and Clearance. To cancel a Clearance/CRQ on the scheduled date, advise the ENOC Escalation and Clearance.

9. Emergency Repairs

9.1 Although emergency repairs do not require submitting a Clearance, a requester still needs to get a go-ahead. The following procedures must be followed depending on the type of emergency repair situation:

- If a critical system or equipment is down hard with no alternate, this is classified as an Incident and a repair can be made real-time without a Clearance/CRQ. The requester needs to identify services that are down and call ENOC Escalation and Clearance at 1-800-892-9743, 1-415-973-3662, or co. 223-3662. The ENOC will make necessary arrangements and give the go-ahead for repairs.
- If a critical system or equipment is not down, but is not functioning properly and there is a high probability of imminent failure (such as a microwave or fiber link taking errors), a repair can be made without a Clearance if a PG&E Manager has provided written

authorization via email. The requester must call the ENOC and provide the Manager's approval email. If the Manager's approval cannot be issued via email, the requester needs to provide a phone number where the Manager can be reached and the ENOC will call to obtain verbal approval. In some cases, the ENOC may be able to assist with obtaining manager approval. After manager approval is provided, the ENOC will make necessary arrangements and give the go-ahead for repairs.

9.2 See Appendix 2. Urgent, Energency Request Workflow

END of Instructions

Telecom & Network Clearance/Change Request Procedure (G2002)

Definitions

Clearance: Method of requesting and obtaining approval to perform work on specified equipment. See also **CRQ**.

CRQ: Change Request. This term is synonymous with Clearance.

CTCC: Contact Call Centers (aka WFM Routing Team)

DCF: Data Center Facility

DCPP: Diablo Canyon Power Plant

DO: Distribution Operations

ECab: Enterprise Change Advisory Board

ENOC: Enterprise Network Operations Center

ENOC Escalation and Clearance: Members of the ENOC Team that analyze, and perform change management and release management functions for Telecom and Network Services Change Requests (Clearances/CRQs).

GDN: Gas Data Network

UDN: Utility Data Network

ODN: Operational Data Network

ISO: Acronym identifying the “California Independent System Operator” of the California electric transmission grid.

Protection Circuit: A connection over certain communication mediums that connect remote electric protection schemes and equipment.

RMC: Resource Management Center

SMC: Application used by Telecom Network Services and ENOC for documenting changes to IT infrastructure

SME: Subject Matter Expert, an individual with in-depth knowledge and high level expertise in performing a specialized job, task or skill.

Switching: In Electric System terminology, this is the process of cutting equipment in and out of service to protect employees and facilities from harm and/or damage.

TOCOC/GRID: Transmission Operations Center Outage Coordination

TCD: Telecom Circuit Database

Telecom & Network Clearance/Change Request Procedure (G2002)

Implementation Responsibilities	Information Technology (IT) Directors, Managers, Supervisors, and Team Leads are responsible for ensuring that their employees receive, understand, and comply with these procedures.
Governing Document	Telecom Network RFC Clearance Procedure
Compliance Requirement/ Regulatory Commitment	NA
Reference Documents	
Appendices	Appendix 1. Change Process Workflow Appendix 2. Urgent, Energency Request Workflow Appendix 3. Release Management Process Flow Appendix 4. Example Telecom CHANGE Request Form Appendix 5. Telecom Clearance Form Field Descriptions Appendix 5. Telecom Clearance Form Field Descriptions Appendix 6. Telecom Request for Approval Email Appendix 7. Telecom Request for Approval Email
Attachments	NA

Telecom & Network Clearance/Change Request Procedure (G2002)

Document Recision

This procedure supersedes G2002 Telecom Clearance Procedures.

Approved By

Stacey Wysocki, Manager, ENOC

Sheryl Whaley, Supervisor, ENOC

Document Owner

Sheryl Whaley, Supervisor, ENOC

Document Contact

Sheryl Whaley, Supervisor, ENOC

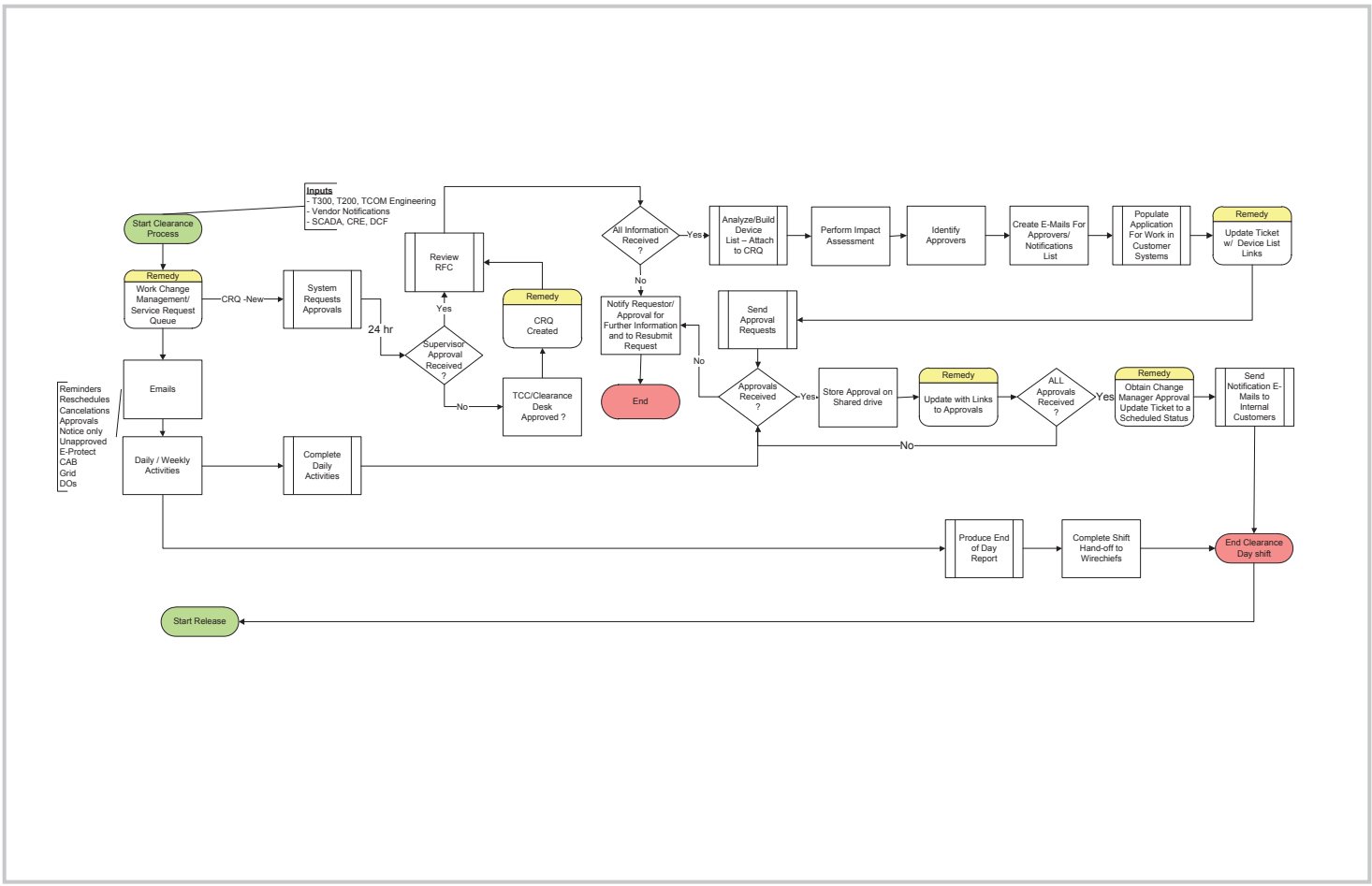
Jeff Wong,Sr Network Analyst, ENOC Escalation & Clearance

Revision Notes

Where?	What Changed?
Entire document	This procedure replaces G2002 Telecom Clearance Procedures which has been edited and reformatted in this GDI format.

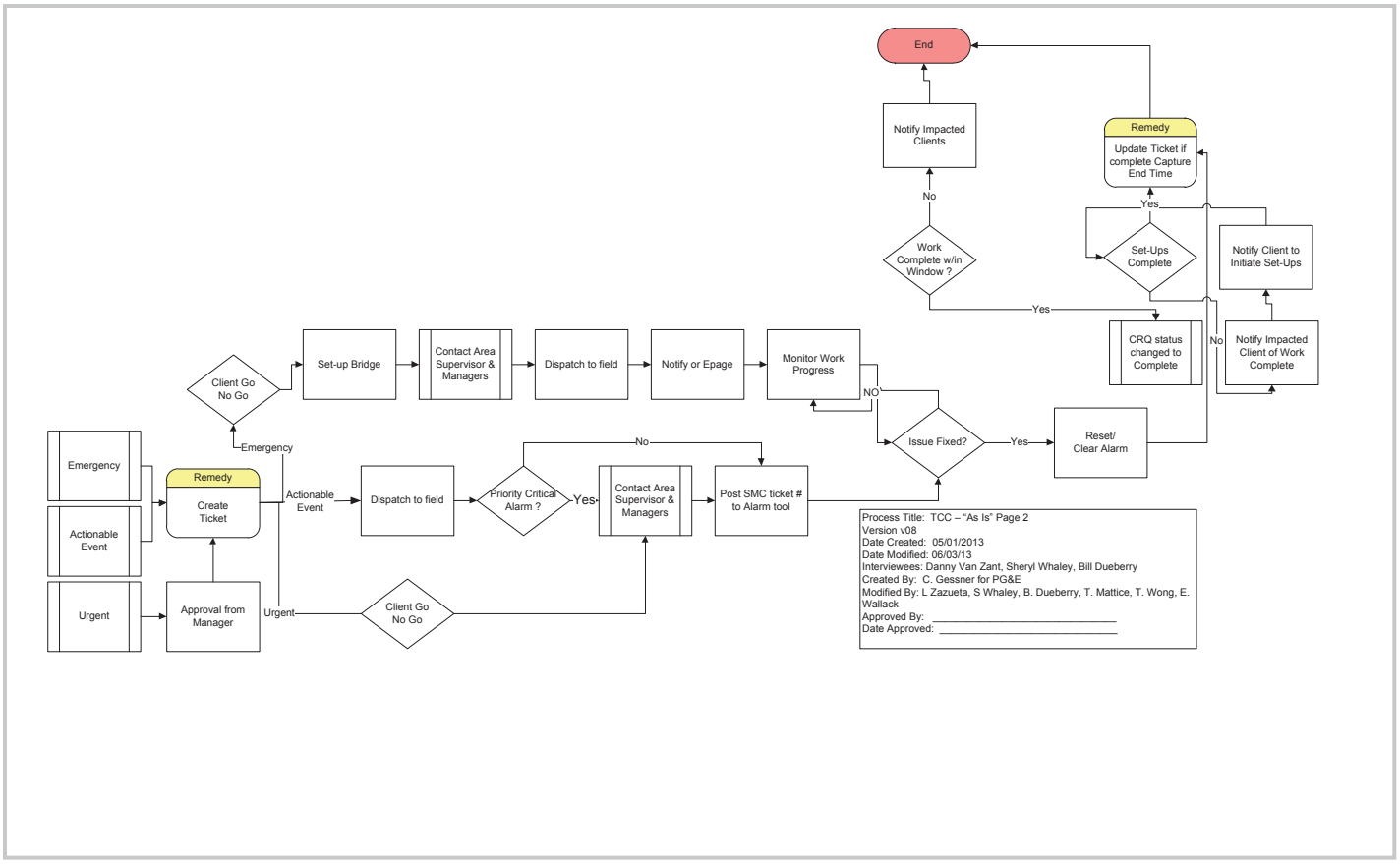
Telecom & Network Clearance/Change Request Procedure (G2002)

Appendix 1. Change Process WorkFlow



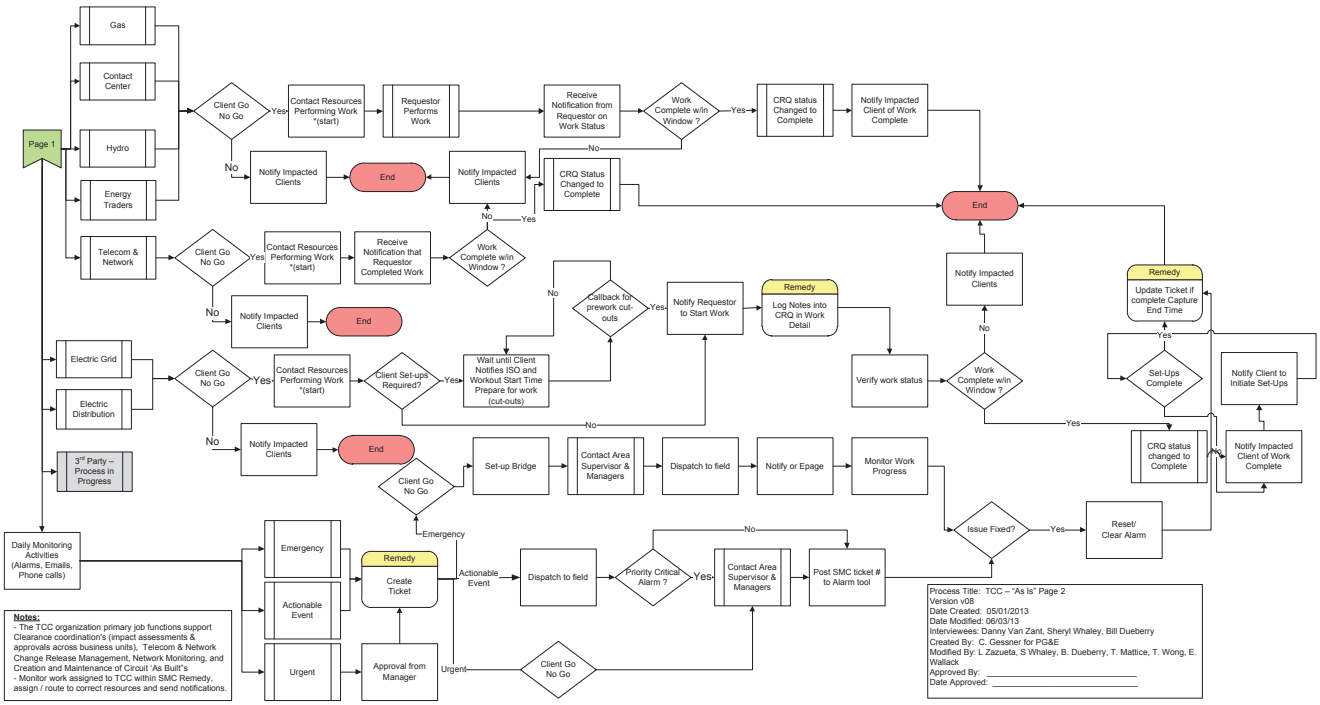
Telecom & Network Clearance/Change Request Procedure (G2002)

Appendix 2. Urgent, Energency Request Workflow

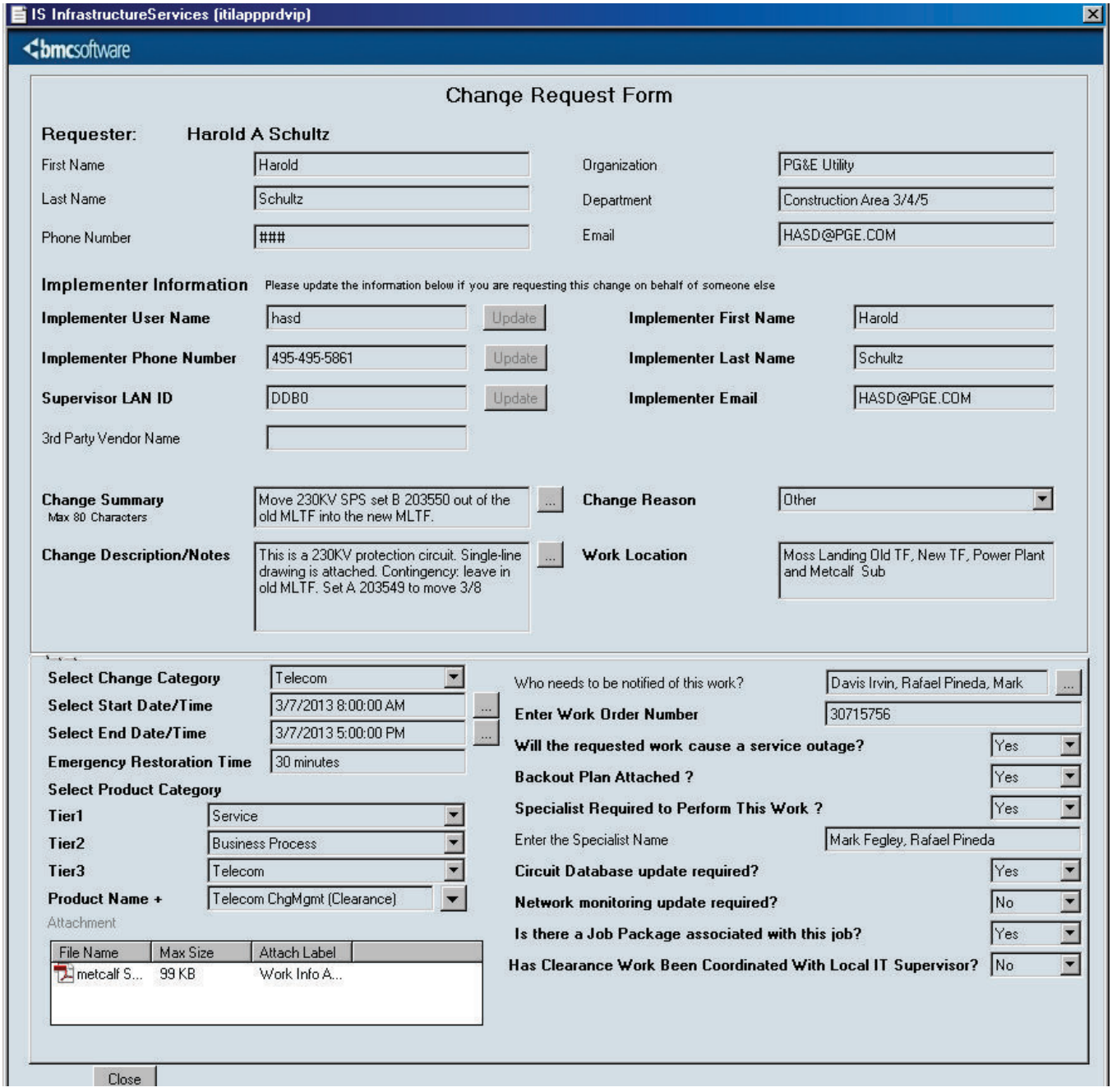


Telecom & Network Clearance/Change Request Procedure (G2002)

Appendix 3. Release Management Process Flow



Appendix 4. Example Telecom CHANGE Request Form



Telecom & Network Clearance/Change Request Procedure (G2002)

Appendix 5. Telecom Clearance Form Field Descriptions

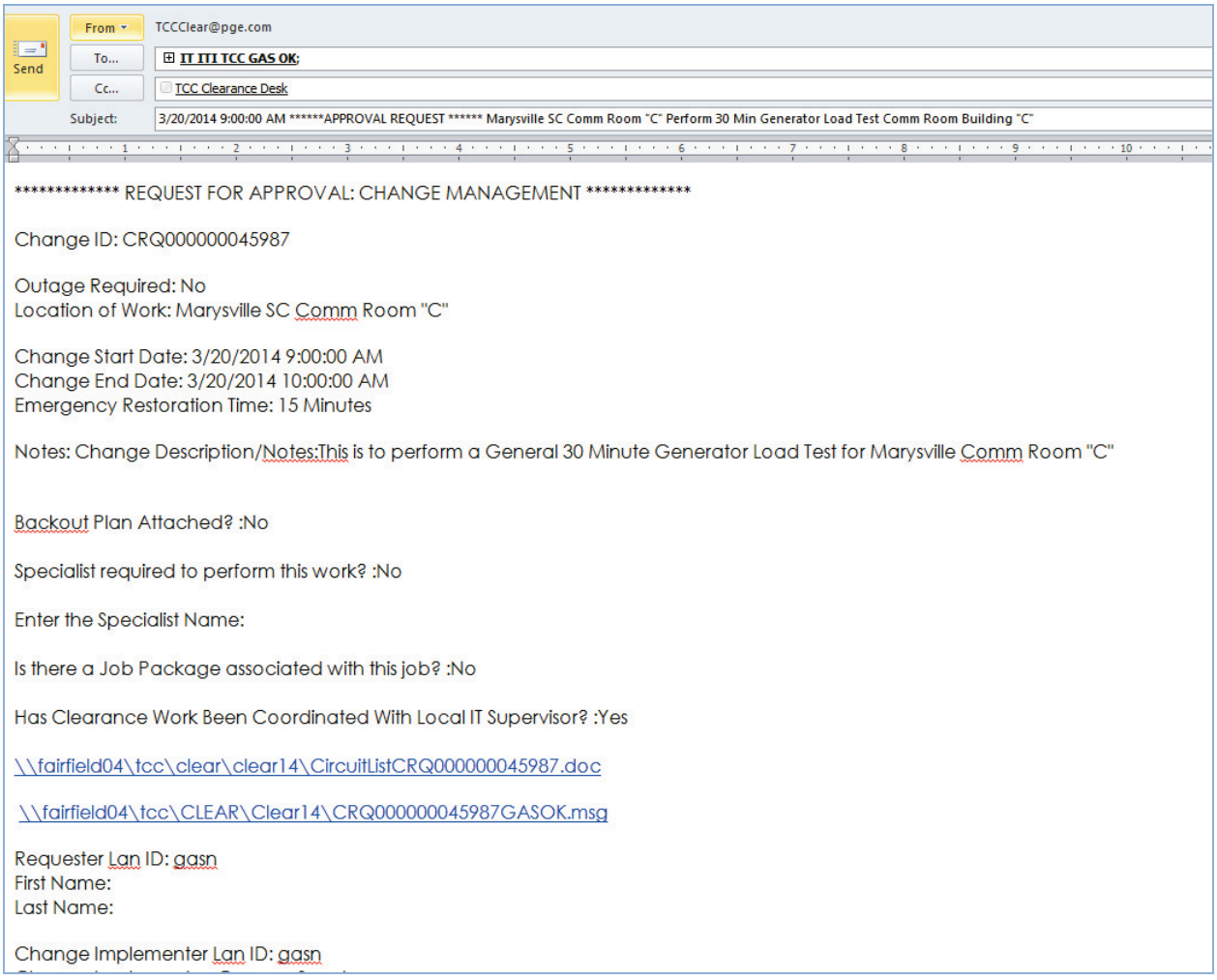
All fields must be completed by the Requester.

Work Location	Location where the change will be performed
Select Change Category ***Note that Network requires Telecom to be selected.***	For Telecom or Network change requests, ***always select Telecom from the dropdown***
Select Start Date/Time	Start Date and Time for the change
Select End Date/Time	End Date and Time for the change
Emergency Restoration Time	Amount of time needed to restore services if problems are encountered with the change request.
Select Product Category	The product categories are associated with the Telecom Change Category field and cannot be changed. 
Who needs to be notified of work?	Additional names and/or groups that need to be notified about this work and added to the notification email outside the normal ENOC notifications (for example, Project Manager.)
Enter Accounting Number	A 7- or 8- digit accounting number must be included on any clearance that will impact Distribution SCADA. A PCC number will not be accepted by the DO AFW tool.
Will the requested work cause a service outage?	Indicates whether or not this change will cause any infrastructure to go down.
Is there a back out plan?	Indicates if a back out plan is attached to the change
Is a Specialist required to perform this work? If so, provide name.	Indicates if a Specialist is required and provides the name of the specialist for the change
Is a circuit database update required?	Indicates if Telecom Circuit Database will be required for this change.
Is Network monitoring	Indicates if Network Monitoring will be required for this

Telecom & Network Clearance/Change Request Procedure (G2002)

update required?	change.
Is there a job package associated with this job?	Indicates if there is a job package for this change.
Has clearance work been coordinated with local IT supervisor?	Indicates local coordination has been conducted so that end users or clients impacted by the change are aware of the upcoming change.
Attachment	This attachment should provide additional details related to this change. (Only 1 attachment can be uploaded so if there are multiple documents provide the documents in a folder on a network share and then provide a link to that folder in the document you upload.)

Appendix 6. Telecom Request for Approval Email



Send
From TCCClear@pge.com
To... IT ITI TCC GAS OK;
Cc... TCC Clearance Desk
Subject: 3/20/2014 9:00:00 AM ******APPROVAL REQUEST ****** Marysville SC Comm Room "C" Perform 30 Min Generator Load Test Comm Room Building "C"

********** REQUEST FOR APPROVAL: CHANGE MANAGEMENT **********

Change ID: CRQ000000045987

Outage Required: No
Location of Work: Marysville SC Comm Room "C"

Change Start Date: 3/20/2014 9:00:00 AM
Change End Date: 3/20/2014 10:00:00 AM
Emergency Restoration Time: 15 Minutes

Notes: Change Description/Notes:This is to perform a General 30 Minute Generator Load Test for Marysville Comm Room "C"

Backout Plan Attached? :No

Specialist required to perform this work? :No

Enter the Specialist Name:

Is there a Job Package associated with this job? :No

Has Clearance Work Been Coordinated With Local IT Supervisor? :Yes

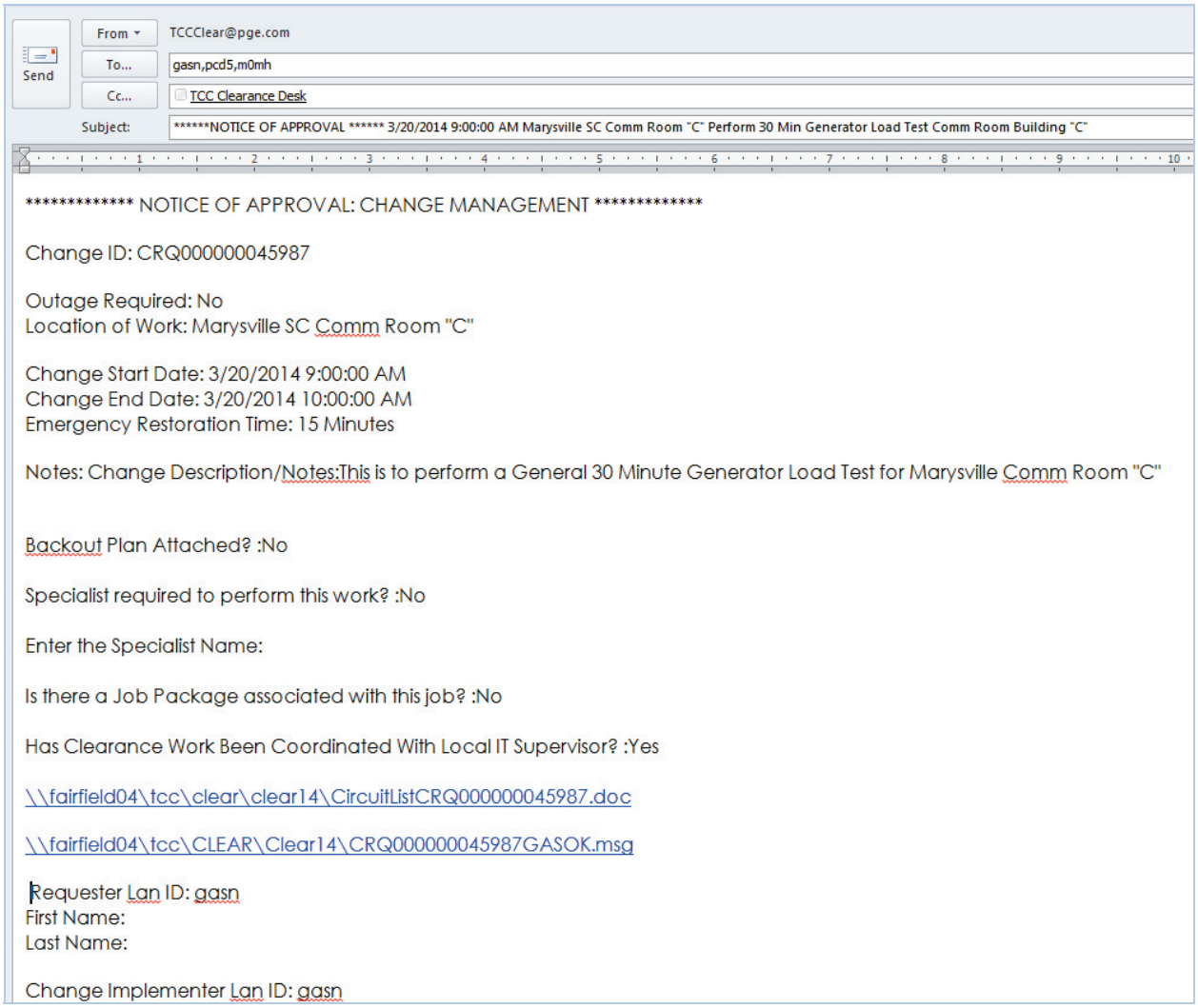
\\fairfield04\tcc\clear\clear14\CircuitListCRQ000000045987.doc

\\fairfield04\tcc\CLEAR\Clear14\CRQ000000045987GASOK.msg

Requester Lan ID: gasn
First Name:
Last Name:

Change Implementer Lan ID: gasn

Appendix 7. Telecom Request for Approval Email



Send

From TCCClear@pge.com

To... gasn,pcd5,m0mh

Cc... TCC Clearance Desk

Subject: ******NOTICE OF APPROVAL ****** 3/20/2014 9:00:00 AM Marysville SC Comm Room "C" Perform 30 Min Generator Load Test Comm Room Building "C"

********** NOTICE OF APPROVAL: CHANGE MANAGEMENT **********

Change ID: CRQ000000045987

Outage Required: No
Location of Work: Marysville SC Comm Room "C"

Change Start Date: 3/20/2014 9:00:00 AM
Change End Date: 3/20/2014 10:00:00 AM
Emergency Restoration Time: 15 Minutes

Notes: Change Description/Notes:This is to perform a General 30 Minute Generator Load Test for Marysville Comm Room "C"

Backout Plan Attached? :No

Specialist required to perform this work? :No

Enter the Specialist Name:

Is there a Job Package associated with this job? :No

Has Clearance Work Been Coordinated With Local IT Supervisor? :Yes

\\fairfield04\tcc\clear\clear14\CircuitListCRQ000000045987.doc

\\fairfield04\tcc\CLEAR\Clear14\CRQ000000045987GASOK.msg

Requester Lan ID: gasn
First Name:
Last Name:

Change Implementer Lan ID: gasn

Docket:	A.17-04-010
ORA Expert Witness:	Cameron Reed
Date:	November 22, 2017

Office of Ratepayer Advocates

Attachment E

PG&E Response to ORA Data Request No. 3

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_003-Q01		
PG&E File Name:	CLEC_DR_ORA_003-Q01		
Request Date:	October 25, 2017	Requester DR No.:	ORA-PG&E-3
Date Sent:	November 1, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Niki Bawa

QUESTION 1

In PG&E's response to ORA DR 1 Question 3, PG&E stated in CLEC_DR_ORA_001-Q03 that "[c]urrent plans involve utilizing out of band equipment via a unique VPN to monitor CLEC telecom equipment."

Please answer the following regarding this quote:

a. What does PG&E mean by out-of-band? In answering this question, include a definition of out-of-band that PG&E utilizes to distinguish out-of-band equipment from in-band or any other equipment.
b. Specify in detail the equipment PG&E defines as out-of-band equipment?
c. Will PG&E accomplish its planned out-of-band monitoring using a different transmission technology (i.e. LTE, Microwave) than the in-band network connection? If yes, what transmission technology does PG&E plan to use?

ANSWER 1

a. Out-of-band data is data transferred through a stream that is independent from the separate main in-band client traffic data stream.

b. Out-of-band equipment would be defined as any equipment or portion thereof that is not carrying the main client data carrying data stream.

c. Yes, in certain CLEC client network designs, out-of-band technology may be utilized for CLEC client network equipment monitoring connectivity. Conceptually, out of band monitoring could be accomplished via cellular modem.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_003-Q02		
PG&E File Name:	CLEC_DR_ORA_003-Q02		
Request Date:	October 25, 2017	Requester DR No.:	ORA-PG&E-3
Date Sent:	November 1, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Niki Bawa

QUESTION 2

In PG&E's response to ORA DR 1 Question 13, PG&E stated in CLEC_DR_ORA_001-Q13 that "PG&E's Enterprise Network Operations Center (ENOC) will utilize the same network monitoring platform that is currently being utilized to monitor the Utility gas and electric networks."

Please answer the following:

a. What kind of system (i.e. hardware, software, cloud based) is the network monitoring platform?

b. Does PG&E's network monitoring platform have any control or administrative permissions to make configuration changes to the network equipment on PG&E's Utility gas and electric network?

ANSWER 2

a. The primary telecom alarm monitoring platform PG&E uses resides on PG&E owned servers at PG&E data centers.

b. Users with proper credentials can use the network monitoring platform application to make configuration changes to network equipment on PG&E Utility gas and electric networks.

PACIFIC GAS AND ELECTRIC COMPANY
Competitive Local Exchange Carrier (CLEC)
Application 17-04-010
Data Response

PG&E Data Request No.:	ORA_003-Q03		
PG&E File Name:	CLEC_DR_ORA_003-Q03		
Request Date:	October 25, 2017	Requester DR No.:	ORA-PG&E-3
Date Sent:	November 1, 2017	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	David Wright	Requester:	Niki Bawa

QUESTION 3

In PG&E's response to ORA DR 1 Question 13, PG&E stated in CLEC_DR_ORA_001-Q13 that "The CLEC telecom network will appear on different screens, network maps, and tables than the Utility gas and electric networks."

Please answer the following:

a. How will the network maps and tables be generated?

b. If any data is stored to create network maps and tables, will CLEC network data and Utility network data be stored in separate databases (i.e. databases that are separate than the electric and gas databases or device inventories)?

c. Will these databases be encrypted and, if so, please describe in detail the type of encryption that will be used (e.g. symmetric versus asymmetric database encryption, encryption standard used such as AES 128 or AES 256, management of private keys, etc.)

ANSWER 3

a. Telecom network maps can be generated electronically from network monitoring tools and displayed on screens or printed. Telecom network maps may also be created in CAD programs. They can be presented electronically or printed.

b. If the CPCN is approved, PG&E plans to store certain CLEC telecom network maps and tables and Utility telecom network maps and tables in shared databases.

c. These databases will be encrypted. Details of encryption and specific database management techniques are confidential; disclosure could pose a threat to the security of the PG&E network.

Docket:	A.17-04-010
ORA Expert Witness:	Cameron Reed
Date:	November 22, 2017

Office of Ratepayer Advocates

Attachment F

Excerpt from A.15-09-001 Supporting Attachments to ORA's Report on Results of Operation for PG&E's Test Year 2017 General Rate case – PG&E Response to ORA Data Request 25, Question 11

Docket:	:	A.15-09-001
Exhibit Number	:	ORA-3-Atch1
Commissioner	:	M. Picker
ALJ	:	S. Roscow
Witness	:	N. Skinner

OFFICE OF RATEPAYER ADVOCATES
CALIFORNIA PUBLIC UTILITIES COMMISSION

Report on the Results of Operations for Pacific Gas and Electric Company Test Year 2017 General Rate Case

Safety, Risk and Integrated Planning

Supporting Attachments

San Francisco, California
April 8, 2016

PACIFIC GAS AND ELECTRIC COMPANY
2017 General Rate Case Phase I
Application 15-09-001
Data Response

PG&E Data Request No.:	ORA_025-Q11		
PG&E File Name:	GRC-2017-PhI_DR_ORA_025-Q11		
Request Date:	October 2, 2015	Requester DR No.:	ORA-PG&E-025-TCR
Date Sent:	October 27, 2015	Requesting Party:	Office of Ratepayer Advocates
PG&E Witness:	Anil Suri & Eric Back	Requester:	Tom Roberts

EXHIBIT REFERENCE: PG&E-4, CHAPTER 13

SUBJECT: GENERAL MWC 06 QUESTIONS

QUESTION 11

Table 13-1 shows how projects proposed in chapter 13 map to risk register IDs. Explain how these risks rank within all risks PG&E faces, as determined in this GRC and the recent GT&S application A.13-12-012, using the complete risk register and supporting workpapers.

ANSWER 11

Attachment GRC-2017-PhI_DR_ORA_025-Q11Atch01 contains all the risks on PG&E's risk register (including gas and electric transmission related risks). The data is based on a query of the Enterprise Compliance Tracking System (ECTS) database that was run on October 9, 2015. The attachment aligns with the risks and related scoring that was included in the 2015 Session D which is part of PG&E's integrated planning process. However, because the register is always evolving and the LOBs are expected to update their risk registers on a regular basis as data and risk evaluations mature, there may be differences between the attachment and prior versions of the risk register. The attachment provides the following information:

- Risk Profile ID -- ECTS tracking number
- Risk LOB -- The line of business that owns the risk
- Risk Name
- Risk Description
- Risk score as calculated using the Risk Evaluation Tool 2.1 (RET2.1)
- EO Risk Designation – This designation is unique to Electric Ops and does not exist in the ECTS database. This column includes the designations from Table 13-1 of Exhibit (PG&E-4), Chapter 13 so ORA can identify how the risks in Table 13-1 rank against all the risks PG&E faces.

The RET 2.1 model used in the 2017 GRC is a newer version than the risk model used in the 2015 GT&S application. It is not appropriate to rank risks using the risk scores populated in the GT&S case and risks evaluated using the RET 2.1 model. See response to ORA11-Q1 for a description of the differences between the two models.

Additionally, risk register information related to gas distribution, electric distribution and energy supply can be found in the workpapers supporting Exhibit (PG&E-3), Chapter 3, Exhibit (PG&E-4), Chapter 2 and Exhibit (PG&E-5), Chapter 2, respectively.

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
258311	Safety and Shared Services	Contractor Safety Program	Failure to comply with the pre-qualification and field processes of the Contractor Safety Standard and LOB Procedures may result in serious injury and/or fatalities.	987	
258404	Safety and Shared Services	Employee Safety Program	The inability to fully identify, evaluate, and control workplace hazards may result in serious injury or loss of life for employees.	979	
251782	Gas Operations	TRA001 - Catastrophic Pipeline Failure - External Corrosion	Rupture of transmission pipeline due to external corrosion may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public or employee safety, prolonged outages, property damages and/or significant environmental damage.	807	
251670	Gas Operations	TRA004 - Catastrophic Pipeline Failure - Manufacturing Related Defects	Longitudinal rupture of transmission pipe may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public safety, significant property damage, wide-scale/prolonged outages.	807	
312431	Gas Operations	TRA008 - Catastrophic Pipeline Failure - Internal Corrosion	Rupture of transmission pipeline due to internal corrosion may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public or employee safety, prolonged outages, property damage.	807	
251665	Gas Operations	TRA003 - Catastrophic Pipeline Failure - Welding / Fabrication Related - Pre-1962 Construction with Land Movement	Circumferential rupture of vintage construction pipe (pre-radiographic pre-1962 girth welds, wrinkle bends, dresser couplings, miter bends, etc.) in known regions of geo-hazards and localized landslide zones may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public safety, significant property damage, wide-scale/prolonged outages.	806	
251726	Gas Operations	STO016 - Internal Corrosion and/or Erosion - Pipeline	Rupture of pipeline due to internal corrosion and/or erosion may result in loss of containment, and/or uncontrolled gas flow that may lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damage and/or environmental damage.	804	
252753	Electric Operations	Wildfire	PG&E assets may initiate a wildland fire that is not easily contained and that endangers the public, private property, sensitive lands, and/or leads to long-duration service outages.	626	
389522	Gas Operations	DMS045 - Incorrect Operations - Cross Bore in Urban Area	Third party sewer clearing may result in damage to distribution pipeline, loss of containment, migration of gas with ignition leading to significant property damage or public safety issues. (Multiple homes or buildings - e.g. downtown San Francisco)	617	
318024	Gas Operations	CP019 - Third Party/Mechanical Damage - Vandalism	The risk of vandalism or terrorist attack at facility may result in personal safety, loss of service, loss of containment, and/or equipment damage.	596	
251563	Information Technology	Cybersecurity	Introduction of malware or execution of commands by authorized and unauthorized users or hackers, use of infected removable media, exposure to phishing, visitation to infected websites, or exploitation of remote connections may lead to the disruption of the confidentiality, integrity, and/or availability of business control applications, computing, data, or networks.	586	
312893	Gas Operations	TRA012 - Catastrophic Pipeline Failure - Weather Related & Outside Forces - Land Movement	Pipeline failure due to land movement associated with seismic activity, flooding, or other geo-hazards (e.g., subsidence, soil creep, fault creep, liquefaction) may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public safety, significant property damage, wide-scale/prolonged outages.	579	
318147	Gas Operations	MC032 - Weather Related/Outside Forces - Seismic	The risk of failure of a station to perform its pressure control function from flooding or seismic event causing downstream under or over-pressure events.	573	
318045	Gas Operations	CP022 - Weather Related/Outside Forces - Seismic (Manned)	The risk of a 6.7 earthquake may result in loss of service, loss entire compressor station (Hinkley and Los Medanos), and ignition.	553	
317677	Gas Operations	CP008- Welding/Fabrication Related	The risk of poor construction practices may result in loss of containment and loss of service.	551	
317785	Gas Operations	CP012 - Manufacturing Defects	The risk of equipment failures from poor design or manufacturing process may result in loss of service and possible loss of containment.	551	
251721	Gas Operations	MC001- Incorrect Operations - LoC LP Distribution	The risk of an overpressure event caused by incorrect operation of low pressure distribution assets may result in failure of downstream assets with loss of containment	551	
252017	Gas Operations	MC015 - Equipment Related - LoC Complex/Simple Station	The risk of an overpressure event caused by equipment failure in a complex/simple station may result in failure of downstream customer assets with loss of containment	551	
251823	Gas Operations	STO026 - Weather and Outside Forces - Seismic	Loss of withdrawal platform, buildings and equipment due to seismic activity/earthquake that may result in the loss of containment or ability to provide storage service. This may lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damage.	551	
251756	Gas Operations	CP006- Incorrect Operations	The risk of incorrect operations causing failure or malfunction of critical pressure containing equipment at a manned facility may result potential loss of containment.	548	
318095	Gas Operations	MC016 - Equipment Related - LoC LP Distribution	The risk of an overpressure event caused by equipment failure in low pressure distribution assets may result in failure of downstream assets with loss of containment	548	
317565	Gas Operations	GSO001 -Failure to Meet Core Customer Demand for Design Standard Abnormal Peak Day (APD)	The risk of not meeting core customer demands as part of the APD design criteria could result in uncontrolled outages which may lead to gas leakage into customer homes and potential explosions.	537	
251568	Information Technology	IT Operational Continuity	Inability to recover, in an agreed upon time frame, the information, people, processes or systems needed to operate the business may result in operational reliability impacts, prolonged customer service outages, revenue and reputation loss	521	
251416	Customer Care	Distributed Generation	The risk of increased customer-side DG adoption may result in the shift of significant costs to non-adopting customers, increase operational issues in the distribution system, and reduce the value of utility assets over the long term.	438	
385591	Electric Operations	Changing GHG Regulations	Incompatible and/or stringent state and federal GHG regulations may result in increase in costs to customers.	417	
384909	Regulatory Affairs	Case Management	Risk of poor case management or case quality resulting in unfavorable regulatory decision	409	
384929	Regulatory Affairs	Compliance Assurance	Risk of lack of compliance assurance programs that lead to lack of compliance in operations related to regulatory interactions, proceedings, requirements, or directives (assurance) resulting in fines, sanctions or unfavorable decisions or policies.	409	
384919	Regulatory Affairs	Customer Affordability – Rate Design	Risk of unreasonable rate structures or inequitable cost allocations resulting in strain on customer affordability, market distortions or unfair rate structures.	409	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
252698	Electric Operations	Distribution Overhead Conductor Primary	Failure of or contact with, energized electric distribution primary conductor results in public or employee safety issues, significant environmental damage, prolonged outages, or significant property damage.	408	EDOH1
303960	Gas Operations	DMS039 - Excavation Damage, Third Party - Rupture Non At-Fault	Damage to gas distribution facilities from a third party (Non At-Fault) may result in loss of containment leading to significant property damage or public or employee injury or fatality.	406	
252708	Electric Operations	Failure of Substation (Catastrophic)	Complete loss of substation may result in significant wide-scale/prolonged outages, public or employee safety issues, significant environmental damage, or significant property damage.	401	
251139	Electric Operations	Hydro System Safety - Dams	The failure of a PG&E dam that may result in significant damage to third parties, the environment and PG&E.	349	
312856	Gas Operations	TRA011 - Incorrect Operations - Over pressurization	Over pressurization, pipeline failure due to incorrect operations by PG&E's staff or contractors may result in loss of containment and/or uncontrolled gas flow that can lead to impact on public or employee safety, prolonged outages due to lack of redundancy on radial feeds, property damage.	348	
284579	Electric Operations	Insider Threat	An employee or contractor uses their PG&E access and company knowledge to gain unauthorized access to steal critical PG&E information. Such unauthorized access or theft may be used to inflict damage, make facilities or systems inoperable, or provide proprietary or valuable company information to other unauthorized parties.	326	
312423	Gas Operations	TRA009 - Stress Corrosion Cracking	Rupture of transmission pipeline due to stress corrosion cracking (SCC) may result in the uncontrolled flow of gas that can lead to significant impact on public or employee safety, prolonged outages due to lack of redundancy on radial feeds and additional SCC-related investigations that would occur post-incident, property damage.	326	
251762	Gas Operations	Gas Compliance Performance Risk	Systemic non-compliance within an LOB resulting from not having an effective compliance program and ethical culture.	316	
252073	Gas Operations	MC004- Incorrect Operations - Complex Stations	The risk of an overpressure event caused by incorrect operation of a local transmission complex station may result in failure of downstream assets with loss of containment	313	
252083	Gas Operations	MC006- Incorrect Operations - Backbone (PLS) Stations	The risk of an overpressure event at complex stations (backbone / PLS stations) caused by incorrect operations may result in damage to downstream assets with loss of containment	313	
390631	Gas Operations	MC010 - Incorrect Operation - Terminal/Large Complex	The risk of an overpressure event at a terminal or large complex station caused by incorrect operations may result in damage to downstream assets with loss of containment	313	
252012	Gas Operations	MC014- Welding/Fabrication - Overpressure Complex Station	The risk of an overpressure event caused by design or fabrication issues a local transmission complex station may result in failure of downstream assets with loss of containment	313	
251868	Gas Operations	STO017-External Corrosion-Pipeline	Rupture due to external corrosion of the pipeline which may result in the loss of pipeline isolation and access as well as an uncontrolled flow or lost production. This may lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	313	
252068	Gas Operations	MC003- Incorrect Operations - LoC Simple Stations	The risk of an overpressure event caused by incorrect operation of a local transmission simple station may result in failure of downstream assets with loss of containment	312	
252007	Gas Operations	MC013 - Welding/Fabrication - LoC Simple Station	The risk of an overpressure event caused by design or fabrication issues at a local transmission simple station may result in failure of downstream assets with loss of containment	312	
391565	Gas Operations	Records Management (Enterprise Shared Risk)	Not implementing fully an effective records & information management program and controlling data quality may result in the failure to construct, operate or maintain a safe system. Additionally, inadequate business processes and system controls related to the collection, maintenance and disposition of records and information can result in non-compliance, security gaps and insufficient or inaccurate data for critical decision making.	312	
251858	Gas Operations	STO020-Manufacturing-Pipeline	Rupture of pipeline due to manufacturing may result in loss of containment, and/or uncontrolled gas flow that can lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	312	
385604	Electric Operations	Above-Market Stranded Costs	Regulatory or political resistance to passing along costs to customers associated with previous investments and contractual obligations leads to financial stress on shareholders.	311	
251512	Human Resources	Employee Qualifications	An employee working without meeting legal, regulatory or PG&E-defined requirements designed to demonstrate the appropriate level of competency for a specific job or specific work may result in: -Work procedure errors -Legal or regulatory non-compliance -Cybersecurity breaches -Localized outages -Damage to property or assets belonging to PG&E, another corporation, a government organization or a member of the public	311	
252027	Gas Operations	MC018 - Equipment Related - LoC Complex/Simple Station	The risk of an overpressure event caused by equipment failure in a local transmission simple/complex station may result in failure of downstream assets with loss of containment	311	
390707	Gas Operations	MC019 - Equipment Related - Backbone (PLS) Stations	The risk of an overpressure event at complex stations (backbone / PLS stations) caused by equipment failure may result in damage to downstream assets with loss of containment	311	
390701	Gas Operations	MC036 - Equipment Related - Terminal/Large Complex	The risk of an overpressure event at a terminal or large complex station caused by equipment failure may result in damage to downstream assets with loss of containment	311	
332465	Customer Care	Meter Technology Lifecycle	Risk of premature meter failure, wavelength interference or service disruption may result in loss of ability to read meters, loss of energy usage information, negative reputational impact or adverse financial impact.	311	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
251838	Gas Operations	STO012 - Erosion - Meters	Erosion of orifice plates that compromises measurement may result in uncontrolled flow and release of gas. This may lead to a significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	311	
317363	Gas Operations	STO015-Erosion-Valves	Erosion of valves may result in uncontrolled flow and release of gas. This may lead to a significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	311	
317373	Gas Operations	STO018-Fatigue-All Segments	Failure of pipeline, equipment, and pipeline controls due to fatigue from internal pressure cycling or vibration may result in loss of containment. This may lead to significant impact on public or employee safety, outages, property damages and/or environmental damage.	311	
390371	Gas Operations	TRA016 - Equipment Related - Over-Pressure Event	Equipment related defect resulting to an OP event downstream causing loss of Containment at a customer facility.	311	
317655	Gas Operations	CP001- External/Internal Corrosion	The risk of through wall leaks in storage injection piping from internal corrosion (discharge side) may result in loss of containment, loss of service and reliability.	310	
251873	Gas Operations	CP002- External Corrosion - Under Pipe Insulation	The risk of through wall leaks from external corrosion forming beneath pipe insulation material may result in loss of service and loss of containment.	310	
251883	Gas Operations	CP005- Manufacturing Defects - Pipe Quality	Loss of containment or reduction in operating pressure due to pipe of unknown or suspect quality (Topock, Hinkley, and station side of Kettleman) or defect resulting from poor manufacture or design practices.	310	
251900	Gas Operations	CP010 - Internal Corrosion & Erosion	The risk of through wall leaks in storage processing, withdrawal piping and pressure vessels from internal corrosion or erosion may result in loss of containment, loss of service, and reliability.	310	
318017	Gas Operations	CP018 - Stress Cracking Corrosion	Deliberate acts of misconduct or unintentional errors by employees or agents that are concealed or deliberately not reported may result in public or employee safety issues, large and prolonged outages, significant property damage, and regulator and public	310	
251691	Gas Operations	DMS005 - Material or Weld - Plastic (System Safety)	Aldyl-A pipe material failure may result in loss of containment (body of pipe crack), gas migration and ignition leading to significant property damage or public safety issue.	310	
251686	Gas Operations	DMS008 - Incorrect Operations - Cross Bore in Suburban Area	Third party sewer clearing may result in damage to distribution pipeline, loss of containment, migration of gas with ignition leading to significant property damage or public safety issues. (Isolated incident - single residence)	310	
251731	Gas Operations	STO003 - Construction by 1st & 2nd Party - Reservoir	Loss of reservoir integrity due to 1st and 2nd party drilling through storage field or reworking 1st and 2nd Party well that may result in an improper completion of the well or uncontrolled flow or loss containment with ignition source that can lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	310	
251853	Gas Operations	STO019-Third Party Damage - Pipeline	Rupture of pipeline due to mechanical damage by 3rd party may result in the loss of pipeline isolation and access as well as uncontrolled flow and loss in production. This may lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	310	
313145	Gas Operations	STO030 - 1st, 2nd, 3rd Party-All Segments	Rupture of pipeline or uncontrolled flow from other storage assets due to 1st, 2nd, and 3rd Party damage caused by equipment/vehicles who may not have followed work procedures that may result in uncontrolled flow of gas, outages or replacement of gas supply. This may lead to major impact on public or employee safety, outages or replacement of gas supply, property damage and/or minor environmental damage.	310	
251772	Gas Operations	TRA006 - Third Party / Mechanical Damage	Rupture of transmission pipe due to mechanical damage by 3rd party may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public or employee safety, prolonged outages, property damage.	310	
252703	Electric Operations	Transmission Overhead Conductors	Failure of or contact with energized electric transmission conductor may result in public or employee safety issues, fires, significant property damage.	310	
251893	Gas Operations	CP007- Incorrect Operations - Odorization	The risk of incorrect operation or maintenance of odorizers may result in over/under-odorization of the gas system, possible equipment damage/failure, and emergency gas leaks calls.	308	
251681	Gas Operations	DMS001 - Excavation Damage, Third Party - Rupture At-Fault due to mismarking by PG&E	Damage to gas distribution facilities from a third party (At-Fault) may result in loss of containment leading to significant property damage or public or employee injury or fatality.	308	
385420	Electric Operations	Portfolio Mix	Implementation of procurement mandates leads to uneconomic portfolio mix and results in inefficient bulk power operations, higher customer cost, and shareholder risk.	308	
385414	Electric Operations	Safety Standards for PPAs	Inadequate consideration of safety when awarding energy procurement contracts results in injury/death to a PG&E employee, a third-party contractor, or the public.	308	
250382	Compliance and Ethics	Company Compliance Performance	Failure to have an effective compliance program and ethical culture in the company may result in severe injuries to the public or employees, substantial impact to the environment, prolonged outages of service, extensive regulatory actions, loss of public trust, or significant financial impacts.	284	
385482	Electric Operations	Electric Grid Restoration	In the event of a system-wide disturbance requiring the deployment of black-start resources, PG&E's restoration plan may not meet current customer or community expectations resulting in trust issues.	283	
252768	Electric Operations	Emergency Preparedness and Response to Catastrophic Events	The risk of inadequate plans and poor response execution to a catastrophic emergency may result in safety concerns, extended outages, regulatory action, and reputational damage. This risk includes business continuity for the enterprise outside of the event.	280	
252803	Electric Operations	Distribution Underground Cable	Failure of or interaction with distribution under ground cables may result in public or employee safety issue or property damage.	245	EDUG2
304081	Gas Operations	DMS014 - Natural Forces	Natural disaster (flood, earthquake) may result in extensive damage to the distribution system due to a fault crossing or breakage of service lines from soft structure failures resulting in loss of containment and ignition leading to property damage and public safety issues.	245	
390688	Information Technology	Network Resiliency	Inability to monitor / control critical sites & assets due to risk of aging network infrastructure and legacy capacity planning methods may lead to the inability of monitoring critical sites and assets and controlling critical gas & electric systems.	242	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
387715	Gas Operations	CCE029 - Material	Purchase and use of unapproved fittings or self-fabricated materials (drips, shop tees) used on indoor meter set assemblies may result in loss containment leading to ignition and safety impact.	237	
387722	Gas Operations	CCE030 - Material Traceability	Lack of traceability on regulators may result in inability to locate and recall material resulting in defective material being left in the field resulting in loss of containment or an overpressurization event which leads to a safety impact.	237	
310112	Electric Operations	Encroachment on EO Assets	Encroachment by third party facilities inside right of way (ROW)/easement may result in public injury or fatality, property damage, increased regulatory scrutiny and interfere with our ability to adequately respond to emergencies and perform maintenance of EO assets.	237	
252793	Electric Operations	Network Components (In Urban/High Density Areas)	Failure of or interaction with underground electric distribution network components in urban areas may result in public or employee safety issue or significant property damage.	237	
252893	Electric Operations	Distribution Overhead Conductor Secondary	Failure of or contact with energized electric distribution secondary conductor may result in public or employee safety issues, fire, or significant property damage.	235	EDOH5
387729	Gas Operations	CCE031 -Other Outside Forces - Building and Meter Interaction	Damage due to building meter interaction (e.g. during an earthquake) may lead to loss of containment and public safety impacts.	235	
317792	Gas Operations	CP013 -Equipment Related - Electrical Systems	The risk of aging electrical equipment at C&P stations may result in worker safety and loss of service.	235	
389571	Gas Operations	DMS053 - Incorrect Operations (Workmanship Traceability)	Inability to identify workmanship in the field when qualification or competency issues arise which results in not being able to identify who completed the work or where the person has previous performed work which may lead to a loss of containment and public or employees safety issues	235	
317595	Gas Operations	GSO003 - Risk of Using Manual Operations	The risk of manual operations could result in customer outages due to insufficient pressure or supply or over pressuring the pipeline due to human error or equipment failure.	235	
251982	Gas Operations	LNG018 - Third-Party Damage - CNG Trailer Transportation Incident	Risk of vehicular incident (e.g., driver failure or unable to avoid, or third party action or equipment failure) may result in collisions or other incidents, and possibly LNG tanker rupture, loss of containment and/or other severe safety impact.	235	
252738	Electric Operations	Transmission Overhead Wood Support Structures	Failure of or interaction with transmission overhead wood poles/structures may result in public or employee safety issue or significant property damage	235	
251917	Gas Operations	CCE007 - Equipment or Other Outside Force - End of Life Failure	End of life failure of gas regulator or, regulator vent debris from insect infestation may result in over pressurizaiton of the customer house line leading to public safety issue.	234	
303890	Gas Operations	CCE011 - Natural Forces (Flood)	Flood event may result in submergence of multiple house regulators and over pressurization of houselines, the release of gas into homes and ignition leading to public safety issues.	234	
251701	Gas Operations	CCE020 - Equipment - Indoor Meter Sets	Failure of indoor meter sets may result in loss of containment, leading to public safety issue.	234	
251676	Gas Operations	DMS004 - Internal Corrosion	Copper service insert in steel or, copper connected to steel, corrodes which may result in loss of containment with gas migration and ignition leading to property damage and public safety impacts.	234	
304089	Gas Operations	DMS015 - External Corrosion - Unprotected Steel Pipe	External corrosion of unprotected (no CP) steel pipe may result in loss of containment leading to migration and ignition.	234	
304104	Gas Operations	DMS022 - Material and Weld - Composit Risers	Internal failue of composite risers (Green Perfection and Powell kit) may result in loss of containment, gas migration and ignition leading to public safety issue.	234	
304110	Gas Operations	DMS023 - Material and Weld - Steel Installed Through the 1950's	Thin wall steel pipe installed through the 1950s is more susceptible to external corrosion may result in loss of containment, gas migration and ignition leading to public safety issue.	234	
389510	Gas Operations	DMS043 - Outside Force - Land Movement Due to Erosion or Subsidence	Land movement due to hillside erosion or sliding may result in pipe overstress, failure and loss of containment with gas migration and ignition leading to safety impact.	234	
389528	Gas Operations	DMS046 - Incorrect Operations - Applicant Installed Facilities	Applicant installed facilities not meeting company requirements may result in loss of containment leading to gas migration leading to public safety issues	234	
251696	Gas Operations	LNG015 - Third-Party Damage - NGV Tank Rupture	Risk of natural gas vehicle (NGV) tank rupture due to integrity management shortfall by customer may result in loss of containment (rupture and high energy release) with severe safety impact, financial loss, loss of reliability (days or weeks long outage), reduced capacity, repair costs.	234	
381234	Safety and Shared Services	Supplier Quality Assurance	Failure to assure quality of materials (i.e. compliance with materials specifications and standards) being supplied to PG&E's construction, maintenance, and operations activities could result in reliability, safety and reputation impacts, as well as increased costs to the company.	234	
320391	Human Resources	Workforce Health	The risk of employees unfit for duty, noncompliant benefits administration or inappropriate disclosure of private employee information may result in: -Injury or death to an employee or member of the public -Legal or regulatory non-compliance -Fines, penalties or increased costs -Reduced employee engagement	234	
284561	Electric Operations	Asset Security	An individual or group commits acts which result in fatalities or inflicts damage making critical facilites inopoerable	229	
384894	Regulatory Affairs	Unfavorable Regulatory Decision - Investigation	Risk of unreasonable fines resulting in lower than expected ROE	216	
252838	Electric Operations	Substation Switches	Failure of, or contact with, substation switch assets which (includes non-protection related devices such as disconnects, air switches, motor operated switches) results in public or employee safety issues, prolonged outages or significant property damage.	215	
252718	Electric Operations	System Integrity Protection Schemes (SIPS)	Unintended operation, non-operation, unavailability of SIPS protection resulting in infrastructure damage, cascading outages, and wide-scale customer interruptions. Additionally, the latter may also result in reduced intertie transfer capability, compliance violations, and uneconomical generation dispatch.	214	
385378	Electric Operations	Voltage Planning and Operation	Extended periods of high voltage on a variety of transmission system equipment leads to pre-mature failures, large outages and dis-allowance of new replacement costs	214	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
252743	Electric Operations	Distribution Overhead Support Structures	Failure of or interaction with distribution overhead wood poles/structures may result in public or employee safety issue or significant property damage	209	
387742	Gas Operations	CCE033 - Other Outside Force - Inaccessibility to system	Installation of roof-top customer connected equipment may result in inaccessibility issues leading to inadequate maintainace resulting in loss of containment resulting in migration into the building resulting in a public safety impact.	202	
389577	Gas Operations	DMS054-Other Outside Forces - Inaccesible Equipment	Installation of roof-top mains and or services may result in inaccessibility issues leading to inadequate mainteance resulting in loss of containment, gas migration into the building and public safety impact	202	
317380	Gas Operations	STO021-Construction-Pipeline	Rupture of pipeline due to vintage construction which may result in loss of containment and/or uncontrolled gas flow. This may lead to significant impact on public safety, property damage, prolonged outages or loss of supply, and/or significant environmental damage.	191	
385585	Electric Operations	Failure of Generation Facility (Catastrophic)	Substantial loss of generation facility may result in reliability issues, public or employee safety issues, significant environmental damage, or significant property damage.	189	
252908	Electric Operations	Critical Equipment Procurement	Inability to timely procure critical equipment or skilled personnel may result in major operational disruptions for Electric Operations and significantly increased cost	187	
251716	Gas Operations	DMS010 - Incorrect Operations - Regulator (Low Pressure)	Low pressure regulating station fails to control pressure may result in high pressure deliver of gas to customers leading to excessive pilot lights and multiple home fires.	184	
313158	Gas Operations	STO029-Third Party Damage-All Segments	Vandalism and/or vehicular damage on above ground pipeline, equipment, wellheads, or valves that may result in damage, over-pressurization, and/or loss of containment. This may lead to impact on public or employee safety, minor outages, property damage and/or minor environmental damage	184	
318134	Gas Operations	MC030 - 3rd Party/Mechanical Damage - Vandalism	The risk of failure of station piping from vandalism/terrorism damage causing may in loss of containment	183	
318037	Gas Operations	CP021 - Weather Related/Outside Forces - Seismic (Unmanned)	The risk of a 6.7 earthquake may result in loss of service, loss entire compressor station (Santa Rosa), and ignition on a CWD.	181	
251863	Gas Operations	STO023-Weather and Outside Force-McDonald Island	Rupture of pipeline and/or failure of well structure due to subsidence at McDonald Island which may result in uncontrolled flow of gas. This may lead to significant impact on public or employee safety, prolonged outages or replacement of supply, property damage, and/or environmental damage	181	
252823	Electric Operations	Transmission Underground Cable and Equipment	Failure of underground transmission assets may result in public or employee safety issues, significant property damage, reduced operational redundancy in critical urban centers, or large-scale prolonged outages	181	
394241	Electric Operations	Contact Voltage	Contact with unintentionally energized PG&E equipment, enclosures, or utility cover plate may result in public or employee fatality or injury, loss of public trust, financial penalty and significant new or expanded regulations	176	
318153	Gas Operations	MC033 - BTU Heating Value	The risk of providing customers with gas that exceeds the BTU limits established in the Chico areas may result in public safety	176	
389565	Gas Operations	DMS052-Material Traceability	Lack of material traceability may result in an inability to locate and recall defective material being left in the field resulting in loss of containment which leads to a public or employee safety issue	175	
387915	Gas Operations	LNG025 - Equipment -CNG Injection Equipment Ops Failure (Safety)	Risk of CNG injection operations failure may result in loss of containment leading to major safety impacts, and possible substantial financial loss, loss of reliability, reduced capacity, significant customer outage.	175	
318103	Gas Operations	MC025 - External Corrosion	The risk of failure of station piping from external corrosion causing gas release with potential risk to public or employee safety.	175	
318159	Gas Operations	MC030.1 - 3rd Party/Mechanical Damage - Vehicular Damage	The risk of failure of station piping from vehicular damage may result in loss of containment	175	
252723	Electric Operations	Substation Transformers and Voltage Regulators	Failure of or contact with energized electric substation transformers may result in public or employee safety issues, significant environmental damage, prolonged outages, or significant property damage.	175	
385386	Electric Operations	Unit Substations	Failure of Unit Sub may result in public or employee safety issues, prolonged outages, and reputational damage to the company	175	
251426	Customer Care	Business Continuity - Contact Centers	The risk of complete loss of phone service to PG&E's contact centers in the event of a Wide Area Network (WAN) failure. Voice over Internet Protocol (VoIP) calls will not reach the contact center, and PG&E may be unable to receive gas leak and/or other hazard calls.	174	
318298	Gas Operations	CP029 - Equipment Related - Hinkley Non-Retrofit compressor Reciprocatting Engine	The risk of Hinkley station retrofitted compressor outage due to any cause may result in loss of service (loss of containment - inherent risk)	174	
304122	Gas Operations	DMS037 - Overbuilds	Overbuilds may result in loss of containment, gas migration into overbuild structure leading to public safety issue.	174	
304129	Gas Operations	DMS038 - Outside Force - Land Movement Due to Creep	Land movement due to creep along seismic fault line may result in pipe over-stress, failure and loss of containment with gas migration and ignition leading public safety issue.	174	
389559	Gas Operations	DMS051 - Co-location of gas and electric facilities	Failure of distribution pipe located at or near electric substations due to operations and incidents at electric substations may result in unsafe work environment (electrified pipe) or loss of containment that can lead to impact on public and employee safety, outages, property damage	174	
252898	Electric Operations	Distribution Underground Line Equipment	Failure of or interaction with energized distribution underground line equipment may result in public or employee safety issues, fire, or property damage (includes capacitors, switches, interruptors, fused switches, and controls)	174	
251446	Customer Care	Failure of Critical Systems	The risk of malfunction or complete failure of systems that are critical or on which the organization is highly dependent to execute day-to-day operations (e.g., CC&B, MDSS, FAS, Telecom/IVR, UIQ, MDMS, CCO WAN or VoIP, Channel of Choice), which may prevent timely processing of customer transactions (e.g., billing, payments, customer-requested work), decreased customer satisfaction and trust, delayed revenue, or public injury.	174	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
252477	Safety and Shared Services	Helicopter Operations	Lack of appropriate oversight and resources may result in the increase of helicopter incidents/accidents, regulatory fines, sanctions, and injury or loss of life for employees and the public.	174	
319470	Electric Operations	Hydro Public Access	Members of the public participating in activities on PG&E lands, facilities and waterways are potentially injured or killed as a direct result of an unplanned hydroelectric operating event or PG&E's failure to reasonably guard or warn consistent with the California recreational use statute against a known dangerous condition, use, structure or activity.	174	
385441	Electric Operations	Hydro Support Infrastructure	Failure of support infrastructure, such as roads, bridges, cableways, and building structures, may result in public and employee safety issues and compliance impacts.	174	
385652	Electric Operations	Hydro Turbine – Generator Systems	Failure of or interaction with turbine and generator systems may result in employee safety issues and reliability issues.	174	
252063	Gas Operations	MC002- Incorrect Operations - LoC HP Distribution	The risk of an overpressure event caused by incorrect operation of high pressure distribution assets may result in failure of downstream assets with loss of containment	174	
252088	Gas Operations	MC007- Incorrect Operations - LoS LP Distribution	The risk of an under-pressure event caused by incorrect operation of low pressure distribution assets with relight risks and unburned pilot gas at customer locations may result to loss of supply, downstream pressure cycles, and ignition	174	
252042	Gas Operations	MC021- Equipment Related - LoS LP Distribution	The risk of an under-pressure event caused by equipment failure in low pressure distribution assets with relight risks and unburned pilot gas at customer locations may result to loss of supply, downstream pressure cycles, and ignition	174	
284553	Electric Operations	Workplace Violence	A disgruntled PG&E employee or contractor uses their PG&E access to enter the workplace and inflict fatal injuries on coworkers and/or customers	174	
251751	Gas Operations	CCE005 - Material or Weld - Inadequate Customer Regulator Design	Inadequate customer regulator design left in service may result in in over pressurization of the customer house line, leading to public safety issue.	173	
320365	Human Resources	Employee Training Governance	The risk of failure to give the right training to the right people at the right time may result in: - Legal or regulatory non-compliance -Fines, penalties or increased costs	173	
259134	Corporate Affairs	Policy Risk	Failure to engage with and educate stakeholders, respond to policy matters and non-compliance with laws and regulations.	171	
252763	Electric Operations	Seismic Resiliency	The occurrence of a large-magnitude seismic event may result in significant damage to PG&E's electric infrastructure and long-duration, large-scale outages.	170	
310155	Electric Operations	Control Room Operational Awareness	Lack of transmission grid operator situational awareness may result in WECC disruption/ system collapse/ cascading outage (incomplete knowledge of system status)	169	
252733	Electric Operations	Substation Protective Relays, Instrument Transformers & Station Batteries	Unintended operation or non-operation of substation protection system may result in large-scale/prolonged outages or significant infrastructure damage	159	
317347	Gas Operations	STO013-Incorrect Operations-Valves	Incorrect valve operations which may result in the failure of control valves to open, close, or shut-in. This may lead to minor impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage. (P50)	158	
258399	Safety and Shared Services	Environmental (Chromium Remediation)	Groundwater contamination from historic operations at Hinkley and Topock has created perceived public health impacts, significant regulatory and financial uncertainly, and reputational impacts. The risk of failure to have constructive stakeholder relationships could lead to increased requirements leading to additional remediation costs, perceived public health concerns, regulatory fines and reputational damage.	156	
312973	Gas Operations	TRA019 - Mechanical Damage - Electric Substation Damage	Failure of transmission pipe located at or near electric substations due to operations and incidents at electric substations may result in unsafe work environment (electrified pipe) or loss of containment that can lead to impact on public and employee safety, outages, property damage	144	
390382	Gas Operations	TRA021 - Material Traceability	The inability to have a systemic process to trace or disseminate information on recalled or obsolete materials for removal or remediation may lead to safety impact.	144	
284567	Electric Operations	Fairfield Security Control	Fairfield Security Control fails to appropriately recognize and respond to available information resulting system damage, failure to alert authorities in a timely manner leading to employee or public safety issues, and making critical facilities inoperable.	141	
384904	Regulatory Affairs	Policy Decisions and Costs	Risk of decisions that create market distortions, uneven playing field or increased operations or commodity costs resulting in strain on customer affordability or loss of	139	
313036	Gas Operations	TRA026 - Equipment Related - Component Failure (Drips, Fittings)	Leak on Transmission component, including drips and fittings that may result in impact on public or employee safety, minor outages and requires valve replacement.	138	
259129	Corporate Affairs	Trust - Company Action or Public Policy Position	Failure to effectively guide potential operational actions or public policy positions.	135	
398991	Corporate Affairs	Trust - Executing the Plans	Failure to execute plans.	135	
384889	Regulatory Affairs	Unfavorable Regulatory Decision - Disallowance	Risk of disallowance of incurred costs resulting in lower than expected ROE	129	
384884	Regulatory Affairs	Unfavorable Regulatory Decsion - Revenue	Risk of underfunding of operations resulting in delays or reductions that affect reliability or the customer experience.	129	
385598	Electric Operations	Bulk Power Operations	Greater levels of market, contractual, and regulatory complexity resulting in potential for the following up through 2020: (1) failure to support system reliability; (2) higher customer cost; and (3) shareholder risk.	128	
250412	Finance	Missed Investor Expectation Risk	Inability to meet investor expectations for financial performance due to unforseen revenue and cost pressures, adverse regulatory outcomes, catastrophic events, inaccurate/incomplete forecasting, or failure to effectively communicate expectations to the investor community. Consequences of not meeting shareholder expectations include: (1) loss in investor confidence in PG&E, (2) damage to management credibility, (3) increase in perceived risk and reduction to stock price (lower P/E), and (4) potential shareholder lawsuits.	128	
387633	Finance	Repairs Inaccuracy	Inaccuracy in repairs data and calculation can result in tax underpayment penalties, financial statement misstatement, inadequate revenue recovery, and impair PG&E's credibility with regulators.	128	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
284011	Nuclear Generation	Nuclear Operations and Safety – Extended Shutdown	An extended shutdown of the Diablo Canyon Power Plant (for longer than three months or with a financial impact greater than $100 million) due to equipment failure, natural disaster, regulatory action, or some other significant event.	126	
252728	Electric Operations	Transmission Overhead Steel Support Structures	Failure of or interaction with transmission overhead steel structures may result in public or employee safety issue, reliability impacts, and/or significant property damage.	117	
251793	Gas Operations	STO005 - Corrosion - Well Casing	Loss of well integrity due to well casing corrosion (internal or external, or stress corrosion cracking) that may result in an uncontrolled flow of gas outside of well casing with ignition source, drinking water contamination, gas migration, or gas loss. This may lead to major impact on public or employee safety, facility outage or net replacement of supply, property damage and/or environmental damage.	114	
251573	Information Technology	Asset Management	Inability to effectively monitor, account for, or demonstrate control of IT assets or asset information may result in prolonged troubleshooting and issue resolution, inefficient use of assets, misguided decisions, miscalculation of cybersecurity risk, Increased exposure to regulatory compliance violations.	113	
310130	Electric Operations	Lack of Real-time Operational Workaround for Loss of Critical Systems	Unexpected loss of operating, control, or monitoring systems may result in system performance degradation, lack of system awareness, and extended restoration times (examples could include EMS, DMS, GIS, etc.)	110	
251164	Nuclear Generation	Nuclear Operations and Safety - Core Damaging Event	Nuclear reactor core-damaging event with the potential for radiological release at the Diablo Canyon Power Plant (Diablo Canyon) due to equipment failure, natural disaster, or some other significant event.	110	
385664	Electric Operations	New Policy & Market Design	Policy decisions or cumulative effect of multiple policies (e.g. 50% RPS, Section 111(d), poor market design, etc.) with unintended consequences results in inefficient market operation. System does not have the required resources that it needs to operate efficiently. Customer costs are unacceptable and PG&E is forced into bankruptcy.	109	
317468	Gas Operations	STO031-Stress Corrosion Cracking-Pipeline	Rupture of pipeline due to stress corrosion cracking (SCC) may result in loss of containment, and/or uncontrolled gas flow. This may lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage.	108	
251828	Gas Operations	STO010-Incorrect Operations - Wells	Failure of well control system during an emergency due to incorrect operations from not following procedures or equipment impairment which may result in uncontrolled gas flow with ignition source. This may lead to significant impact on public or employee safety, and/or prolonged outages or net replacement of supply.	107	
251833	Gas Operations	STO011-Erosion - Wells	Damage to the wellhead due to erosion that may result in loss of well isolation and access or uncontrolled flow with ignition source. This may lead to significant impact on public or employee safety, prolonged outages or net replacement of supply, property damage and/or environmental damage.	107	
251441	Customer Care	Customer Data Breach	The risk of unauthorized exposure or loss of personally identifiable customer information (PII) may result in negative reputational impact, loss of customer satisfaction and trust, or adverse financial impact.	106	
385453	Electric Operations	Hydro Pressure Integrity Systems	Failure of high pressure systems or related valves may result in public or employee safety issues, environmental damage, reliability issues, and cascading infrastructure impacts	104	
385567	Electric Operations	Fossil Fuel Systems	Failure of or interaction with fuel systems may result in public or employee safety issues, environmental damage, and significant property damage.	103	
251987	Gas Operations	LNG024.0 - Equipment -LNG Vaporizer Operations Failure (Safety)	Risk of vaporizer operations failure may result in loss of containment leading to major safety impacts, and possible substantial financial loss, loss of reliability, reduced capacity, customer outage (7k to 20k) along with LNG into pipeline. Highest consequence vaporizer failure.	103	
398996	Corporate Affairs	Load Loss Risk	Failure to address customer load loss leading to challenges in managing the bundled portfolio, customer relationships and potentially stranding assets.	103	
251787	Gas Operations	STO004-Incorrect Operations - Reservoir	Over-pressurization that may result in compromising caprock integrity, gas migration, loss of gas, drinking water contamination, or need to abandon the storage field indefinitely. This may lead to impact on public or employee safety, prolonged outages or net replacement of supply, property damage and/or environmental damage.	103	
312925	Gas Operations	TRA014 - Mechanical Damage - First & Second Party Damage	Failure from transmission pipe resulting from mechanical damage by PG&E (1st and 2nd party damage) may result in the uncontrolled flow of gas that can lead to significant impact on public safety, significant property damage, wide-scale/prolonged outages.	103	
251977	Gas Operations	LNG016 - Third-Party Damage - LNG Tanker Transportation Incident	Risk of vehicular incident (e.g., driver failure or unable to avoid, or third party action or equipment failure) may result in collisions or other incidents, and possibly LNG tanker rupture, loss of containment and/or other severe safety impact.	102	
298557	Gas Operations	LNG017.0 - Third-Party Damage - LNG Tanker Parked (Safety)	Risk of collision of a vehicle or other object with LNG Tanker (Portable Supply Equipment parked) may result in tank rupture, significant loss of containment, fire and/or explosion that could cause severe safety impacts.	102	
324539	Safety and Shared Services	Seismic Tsunami	Risk that facilities managed by Safety and Shared Services are not prepared to handle a catastrophic event, potentially causing safety and operational impacts due building damage.	100	
251345	Regulatory Affairs	Information Management & Analytics	Risk of insufficient data analytics and access resulting in a lack of compliance, accuracy or analytic support for cases.	99	
385407	Electric Operations	Significant Natural Gas Price Increase	Significant increase natural gas prices would result in high gas bills for bundled core gas customer which could result in some customers being unable to pay their bills. Ultimately the crisis could create a gas supply reliability issue, a potential financial issue, as well as a lack of trust with customers.	99	
250407	Finance	Energy Market Risk	Sharp increase in commodity prices resulting in higher electricity and/or gas charges for customers.	98	
385573	Electric Operations	Fossil Chemical Systems	Failure of chemical systems may result in public or employee safety issues, environmental damage, and significant infrastructure (building, pipe, etc.) damage.	98	
385488	Electric Operations	Fossil Turbine – Generator Systems	Failure of or interaction with turbine and generator systems may result in employee safety issues and reliability issues.	98	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
252098	Gas Operations	MC009- Incorrect Operations (System Safety)	The risk of an under-pressure event caused by incorrect operation of high pressure distribution assets with relight risks and unburned pilot gas at customer locations may result to loss of supply, downstream pressure cycles, and ignition	98	
252002	Gas Operations	MC012 - Welding/Fabrication - Overpressure Event (System Safety)	The risk of an overpressure event caused by design or fabrication issues with high pressure distribution assets may result in failure of downstream assets with loss of containment	98	
252022	Gas Operations	MC017- Equipment Related (System Safety)	The risk of an overpressure event caused by equipment failure in high pressure distribution assets may result in failure of downstream assets with loss of containment.	98	
252047	Gas Operations	MC022- Equipment Related - LoS HP Distribution	The risk of an under-pressure event caused by equipment failure in high pressure distribution assets with relight risks and unburned pilot gas at customer locations may result to loss of supply, downstream pressure cycles, and ignition	98	
390735	Gas Operations	MC028 - Stress Cracking Corrosion	The risk of failure of station piping from stress cracking corrosion causing loss of containment may result in public safety.	98	
318122	Gas Operations	MC029 - Internal Corrosion	The risk of failure of station piping from internal corrosion causing loss of containment may result in public safety.	98	
250432	Finance	Raise Sufficient Equity	Inability to access the equity markets to meet a portion of the company's liquidity needs	98	
317389	Gas Operations	STO022-Weather and Outside Force-LM and PC	Rupture of pipeline and/or failure of well structure due to subsidence at Los Medanos and Pleasant Creek which may result in uncontrolled flow of gas. This may lead to significant impact on public or employee safety, prolonged outages or replacement of supply, property damage, and/or environmental damage	98	
251214	Electric Operations	AB 32 / Cap-and-Trade	Insufficient supply of allowances and offsets could lead to extremely high costs to customers.	97	
250397	Finance	Insurance Risk	Inability to purchase sufficient insurance to cover a 1 in 100 year return period loss (liability, property, nuclear, director and officer coverages) may result in significant financial losses for the company.	97	
298592	Gas Operations	LNG026 - Third-Party Damage - ORCA Trlr Transpo Incident	Risk of vehicular incident (e.g., driver failure or unable to avoid, or third party action or equipment failure) may result in collisions or other incidents, and possibly LNG tanker rupture, loss of containment and/or other severe safety impact.	97	
313018	Gas Operations	TRA023 - Third Party / Mechanical Damage - Vandalism	Vandalism and/or vehicular damage on above ground pipeline/equipment, including illegal/nefarious valve operation, may result in damage, over-pressurization, and/or loss of containment that may lead to impact on public or employee safety, minor outages, property damage.	97	
251818	Gas Operations	STO025 - Equipment - Storage Field Facilities	Interruption of power and failure of backup system at the facilities which may result in loss of operation of equipment and monitoring technologies. This may lead to minor impact on public or employee safety, outages or net replacement of supply or property damage. (P50)	95	
253042	Electric Operations	Risk of Non-Compliance	The risk of not using an effective system of internal controls and processes, as part of the compliance program/framework, may result in cease and desist orders and/or the forced shutdown of critical assets and facilities.	82	
313011	Gas Operations	TRA022 - Incorrect Operations	Failures of transmission pipe due to PG&E employees or contractors not following work procedures may result in loss of containment that can lead to impact on public or employee safety, outages, property damages.	82	
310124	Electric Operations	Workforce Planning	Ineffective workforce planning may result in loss of critical knowledge and specialized skills with an associated increased level of serious WPEs/ HEs, delayed restoration, and decreased ability to maintain system assets.	81	
278767	Safety and Shared Services	Material Recall	Failure to maintain proper records and procedures with regards to material recall could potentially lead to PG&E property loss, third party property loss, damage to the environment, compliance failures and loss of life.	79	
251588	Information Technology	Business Adoption & Benefits Realization	Inability to deliver business-required outcomes as a result of inadequate change planning, ongoing lack of capacity to effectively deliver sustainable change, and the misaligned focus on project cost instead of realized business benefits may result in lower return on investment, higher total cost of ownership and inefficient use of organization resources	77	
251224	Electric Operations	Market Flaws / Manipulation	Market flaws or inefficiencies allow manipulation or other undesirable outcomes leading to increases in market prices (i.e. extremely high costs to customers, possible negative financial shareholder impacts).	76	
251746	Gas Operations	LNG012 - Third-Party Damage - Fueling Station Drive Away	Risk of inadvertent dispenser equipment damage by fuel customers (drive off) which is common, may result in loss of containment leading to a fire, extensive safety impact, financial loss, loss of reliability (days or weeks long outage), reduced capacity, repair costs.	74	
252713	Electric Operations	Loss of Transmission Corridor	Loss of critical transmission path may result in inability to serve load, disruption of major generation sources, and significant financial and regulatory penalties (excludes generator station equipment and other Energy Supply assets)	73	
298535	Gas Operations	LNG024.1 - Equipment - LNG Vaporizer Outage (Reliability)	Risk of vaporizer (portable equipment during operation) injection failure due to equipment failure, other outside force, or operator error may result in major loss of supply to customers and possible safety impact, substantial financial loss, along with LNG into pipeline. Highest overall risk of LNG vaporizer outage (excluding highest consequence.	72	
385398	Electric Operations	Substation Bus Structures	Failure of or interaction with substation structures and foundations may result in public or employee safety issue or prolonged outages	69	
390218	Gas Operations	GSO009 - Scheduling Risk	The inability to properly schedule gas may result in regulatory action, gas shortage, and improper/inability to bill.	68	
390477	Customer Care	CC&B Access Controls	Risk of inadequate access controls and system governance may result in customer privacy exposures, financial errors or employee fraud.	66	
398986	Corporate Affairs	Trust - Develop and Maintain the Plans	Failure to develop and maintain appropriate plans.	64	
252878	Electric Operations	Cover-up/ Fraud	Deliberate acts of misconduct or unintentional errors by employees or agents that are concealed or deliberately not reported may result in public or employee safety issues, large and prolonged outages, significant property damage, and regulator and public	61	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
390358	Gas Operations	TRA010 - Weather-Related Outside Force - Water Crossings & Exposed Pipe	Failure of exposed pipeline designed to be under a water crossing due to prolonged scour and debris built up along exposed pipe may result in loss of containment and/or uncontrolled gas flow that can lead to impact on public or employee safety, property damage, outages.	58	
312981	Gas Operations	TRA020 - Weather Related & Outside Forces - Tree Damage	Failure of transmission pipe due to trees damaging the pipe may result in loss of containment and/or uncontrolled gas flow that can lead to significant impact on public safety, significant property damage, wide-scale/prolonged outages.	58	
251436	Customer Care	Loss of Program Administration	The risk of losing critical components of energy efficiency, low-income, demand response, or self generation program administration to a third party may result in reduced customer satisfaction, negative reputational impact, PG&E's failure to achieve key metrics, and / or lack of visibility into impacts on the grid.	55	
310118	Electric Operations	Lack of Transmission Project Delivery	Non-execution of proposed and forecast transmission work projects may result in system performance degradation, reduced system resiliency, and/or un-served load as well as loss of credibility of future transmission proposals	54	
318221	Gas Operations	CP024 - Hinkley Station Non-Retrofitted compressor outtage due to any cause	The risk of outage at Hinkley Station due to any cause on CWD may result in loss of service.	53	
318059	Gas Operations	CP025 - Delevan Station compressor outtage due to any cause	The risk of outage at Delevan Station due to any cause on CWD may result in loss of service	53	
390582	Gas Operations	CP032 - Santa Rosa Station compressor outtage due to any cause	The risk of outage at Santa Rosa Station due to any cause on CWD may result in loss of service	53	
252808	Electric Operations	Substation Circuit Breakers and Switchgear	Failure of or contact with energized substation circuit breakers and switchgear may result in public or employee safety issues, significant environmental damage, prolonged outages, or significant property damage.	53	
251593	Information Technology	Risk of Non-Compliance	Risk of systemic compliance failure in IT's Compliance program could lead to public and employee safety issues, fines, regulatory censure, and inability meet business objectives.	51	
251952	Gas Operations	CCE013 - Natural Forces (Seismic)	Seismic event may result in failure of large diaphragm meters and loss of containment and ignition leading to public safety issue.	50	
250427	Finance	Liquidity Risk	The lack of sufficient liquidity to meet PG&E's financial obligations (liquidity is defined as the availability of cash)	50	
318533	Information Technology	Employee Qualifications	The risk of employees working without meeting legally required qualifications may result in: Safety issues; Work procedure errors	49	
251583	Information Technology	Project Delivery	Inability to deliver business-required outcomes due to inadequate project planning and execution may lead to deployment of lower quality solutions, unmet customer objectives, requirements, or benefits, not delivering on time or within budget	47	
284077	Nuclear Generation	Caisson and Subsurface Structure Removal	Risk associated with demolition and removal of Unit 3 caisson and other underground structures may lead to serious injury, spread of contamination into soils, schedule escalation, funding shortfall/cost over-run, negative public relations, disallowance for imprudent costs, and potential civil judgments	46	
251199	Nuclear Generation	Combined Solid Waste Preparation and Transport	Risk of traffic accident or incident associated with the preparation, loading, and transportation of solid waste from HBPP may result in employee, contractor, and public injuries and fatalities, and/or inadvertent release of radioactive or hazardous industrial materials to the environment.	46	
251578	Information Technology	Performance Monitoring & Reporting	Undesirable outcome resulting from inadequate operational monitoring may result in longer or more frequent system outages and incorrect root cause analysis	46	
387735	Gas Operations	CCE032 - Other Outside Force - Spatial Clearance	MSA in a location with an inadequate spatial clearance in a normal or abnormal operating condition may result in ignition leading to a fire at the meter set and structure damage leading safety impact to the public.	45	
317779	Gas Operations	CP009-Equipment Related - Air Emission Regulation	The risk of existing equipment or technology not being able to be upgraded enough to comply with stricter air emission regulations may result in loss of service and non-compliance.	44	
252162	Safety and Shared Services	Critical Facilities - Data Centers	Failure to maintain/protect critical facility building systems may impact operations creating a safety risk to employees, and business operations. This could potentially impact reliability of gas and electric service, increase costs to PG&E, cause reputational damage, and/or regulatory fines.	44	
317605	Gas Operations	GSO010 - Risk of Multiple Clearances in the same Gas System	The risk of customer outages due to complex operations associated with clearances could result in uncontrolled outages which may lead to gas leakage into customer homes and potential explosions.	43	
251547	Human Resources	Recruiting, Talent Management and Diversity	The risk of non-standardized processes or discrimination in onboarding and off-boarding employees may result in: -Legal or regulatory non-compliance -Fines, penalties or increased costs -Reduced employee engagement	43	
317451	Gas Operations	STO020.1-Manufacturing-Pipeline	Leak in pipeline due to manufacturing may result in loss of containment, and/or uncontrolled gas flow. This may lead to minor impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage. (P50)	43	
383077	Safety and Shared Services	Critical Facility Non-Data Center	Failure to maintain/protect critical facility building systems may impact operations creating a safety risk to employees, and business operations. This could potentially impact reliability of gas and electric service, increase costs to PG&E, cause reputational damage, and/or regulatory fines.	42	
385468	Electric Operations	Hydro In-stream Flow Release (IFR) Valve and Bypass	Failure of or interaction with in-stream flow release valve or bypass systems may result in environmental damage and compliance requirements.	42	
298649	Gas Operations	LNG031 - Insufficient Portable Equipment	Risk of insufficient portable supplies may result in major financial impacts to pipeline projects and decreased service reliability to customers.	42	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
278756	Safety and Shared Services	PCB Oil-Filled Equipment	Failure to develop a long-term plan to identify and replace oil-filled equipment containing PCBs at currently permissible levels (e.g., pole mounted transformers) could result in environmental and reputational impacts if the equipment fails, and/or significant costs if future regulations require removal/replacement.	42	
251947	Gas Operations	CCE004 - Other Outside Force - Third Party Damage - Construction & Redevelopment	Third party damage due to construction & redevelopment may result in loss of containment and ignition leading to public safety issue.	41	
384924	Regulatory Affairs	Customer Affordability – Rate and Bill Volatility	Risk of highly variable rates structures due to changing policy, rate design or revenue awards resulting in strain on customer affordability for certain classes	41	
318496	Corporate Affairs	Cybersecurity	An intentional/unintentional loss of control of information and systems used for gas and electric operations (e.g., SCADA, plant networks, trading, etc.) and business operations (e.g., finance, human resources, back office, etc.) may result in: Life safety events, Operational reliability impacts, Privacy and Intellectual Property Theft, Revenue and reputation loss	41	
390430	Customer Care	Key Vendor Continuity	Risk of key vendor failing to meet obligations for financial or other reasons may result in disruption of PG&E's ability to deliver products and services to our customers	41	
332449	Finance	Natural Hazard Asset Performance	The risk that individual PG&E assets (excluding DCPP) may not be able to sufficiently withstand natural threats, such as a seismic, tsunami, or flood event, and may result in an unacceptable delay in a return to normal operations.	41	
317404	Gas Operations	STO027-Incorrect Operations-Storage Field Facilities	Technology used for monitoring and controlling assets is incorrectly maintained or damaged which may result in loss of well control, manual operations or not being able to operate storage facilities. This may lead to significant impact on outages or net replacement of supply.	39	
251179	Nuclear Generation	HBPP End State	Risk of failure to obtain approval of our End State filing may result in negative impacts to our End State Plan, including potentially significant customer, environmental, and political issues on the disposition of sub-grade structures and soils that will remain after decommissioning.	38	
251431	Customer Care	Management and Execution of Third Party and Customer Contracts	The risk of mis-managing or incorrectly executing third-party contracts associated with regulatory programs and/or customer contracts may result in the misrepresentation of contractual terms and/or program rules, failure to identify fraud, failure to ensure security when relying on third-party vendors, decreased customer satisfaction and trust, or loss/misstatement of revenue.	38	
313031	Gas Operations	TRA025 - Equipment Related - Inoperable Valves	Leak on transmission main line valve and/or inability to operate valve due to equipment failure may result in impact on public or employee safety, minor outages and requires valve replacement.	38	
385447	Electric Operations	Hydro Protection and Control Systems	Unintended operation or non-operation of powerhouse protection, DCS and SCADA systems may result in public and employee safety and reliability issues.	37	
324534	Safety and Shared Services	Use of Non-Approved Material	The risk of a failure to use materials that adhere to PG&E's procurement policy and/or specification requirements for PG&E's construction, maintenance, and operations activities results in business impacts (reliability, safety, reputation)	35	
389535	Gas Operations	DMS047 - Other Outside Forces - Tree Root Damage to Plastic Pipe	Tree Root damage of plastic distribution mains and services may result in loss of containment leading migration and possible public safety impact.	34	
277852	Human Resources	Non-Employee Workforce Program	The risk of an immature / emerging non-employee workforce program with few controls may cause safety, financial or reliability issues	34	
317436	Gas Operations	STO016.1-Internal Corrosion and/or Erosion - Pipeline	Leak in pipeline due to internal corrosion and/or erosion may result in loss of containment, and/or uncontrolled gas flow or lost production. This may lead to minor impact on public or employee safety, outages or net replacement of supply, property damage and/or environmental damage. (P50)	34	
303930	Gas Operations	CCE026 - Equipment Failure - Meter/Regulator	Meter and/or regulator fails to deliver gas to customer may result in loss of service to a large or critical customer shutting down their operations which could lead to a chemical process failure leading to facility damage and injury.	33	
385561	Electric Operations	Fossil High Energy Systems	Failure of high pressure systems or related valves may result in public or employee safety issues, environmental damage, reliability issues, and cascading infrastructure impacts.	33	
252833	Electric Operations	Substation Voltage and Flow Control Equipment	Failure of or contact with energized voltage or flow control equipment may result in public or workforce safety issues, environmental damage, prolonged outages, or significant property damage.	32	SS4
298567	Gas Operations	LNG019.0 - Third-Party Damage - CNG Tube Trailer Parked (Safety)	Risk of collision of a vehicle or other object with CNG Tube Trailer (Portable Supply Equipment parked) may result in vessel damage, significant loss of containment, fire and/or explosion that could cause extensive safety impacts.	32	
298642	Gas Operations	LNG030 - Incorrect Operations - Station Documentation Safety	Risk of incomplete documentation for CNG fueling stations may result in engineering or operations errors that may cause major safety impacts on personnel or the public.	32	
298658	Gas Operations	LNG032.0 - Equipment - Station Compressor and Component (Safety)	Risk of Compressor (Fueling Station) or component material failure may result in pressure/shrapnel that could cause major safety impacts to nearby personnel.	32	
258100	Safety and Shared Services	Supplier Risk – Sole Source Dependence	Failure of a supplier to filfil obligations for goods and/or services, which could lead to project delays, costs to PG&E, reputation damage, disrupted service to customers and degraded reliability	32	
252888	Electric Operations	Transmission Overhead Switches	Failure of overhead transmission switches may result in employee safety issues, prolonged outages, fires, or significant property damage	32	
252853	Electric Operations	Distribution Underground Subsurface and Pad-Mount Transformers	Failure of or contact with energized distribution transformers may result in public or employee safety issues, fire, or property damage.	31	EDUG3
252748	Electric Operations	Distributed Generation	Potential for increased levels of customer-side DG adoption may result in operational issues in the distribution system.	31	PROC12
389553	Gas Operations	DMS050 - Military facilities	Acquired military facilities that have no records and substandard installations may result in health and safety impacts or loss of containment.	31	
250417	Finance	Inadequate Revenue Recovery	Failing to accurately forecast capital or tax costs in a rate case would lead to inadequate revenue recovery.	31	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
298615	Gas Operations	LNG027 - Third-Party Damage - ORCA LNG Safety Parked	Risk of collision of vehicle or other object during transportation with the ORCA (Portable Supply Equipment while stationary) may result in loss of LNG containment and extensive safety impact on personnel or the public.	31	
389516	Gas Operations	DMS044 - Excavation Damage - Unlocatable Stubs	Unlocatable stubs may result in at-fault dig in leading to loss of containment and a public safety impact	30	
251456	Customer Care	Failure to Safeguard Cash	The risk of mismanaging records, equipment or facilities designed to safeguard cash may result in internal or external theft of cash.	30	
317579	Gas Operations	GSO002 - Failure to meet Non-Core CWD Design Standard	The risk of not meeting non core customer demands during any Cold Winter Day Design criteria could will result in more non core customer curtailments.	30	
298621	Gas Operations	LNG028 - LNG Commodity Shortfall	Risk of LNG supply reliability shortfall may result in absence of portable equipment support for construction projects or emergency response, resulting in higher project costs or decreased customer service reliability.	30	
298670	Gas Operations	LNG032.1 - Eqpmt - Combined Sta Compr and Component (Reliability)	Risk of compressor (Fueling Station) material failure may result in reliability risk.	30	
317354	Gas Operations	STO014-Equipment-Valves	Failure of valves to control due to incorrectly or poorly maintained equipment which may result in a well overflow. This may lead to impact on public or employee safety, prolonged outages or net replacement of supply, property damage.	30	
252052	Gas Operations	MC023 - Equipment Related - LoS Simple Station	The risk of an under-pressure event at simple station due to equipment failure may result in loss of supply and downstream pressure cycles.	29	
298631	Gas Operations	LNG029 - CNG Commodity Shortfall (Reliability)	Risk of CNG supply reliability shortfall may result in absence of portable equipment support for construction projects or emergency response, resulting in higher project costs or decreased customer service reliability.	28	
318113	Gas Operations	MC026 - Manufacturing Related Defects	The risk of a pressure reduction or under-capacity event caused by insufficient station documentation to support MAOP validation with potential for relight risks and unburned pilot gas at customer locations may result in loss of service impacting multiple customer locations.	28	
251848	Gas Operations	STO002- Construction by 3rd Party - Reservoir	Construction by a 3rd Party drilling through storage field or reworking 3rd Party well that may result in an improper completion of the well or uncontrolled flow or loss of containment. This may lead to impact on public or employee safety, outages or replacement of supply, and property damage	28	
317460	Gas Operations	STO031.1-Stress Corrosion Cracking-Pipeline	Leak in pipeline due to stress corrosion cracking (SCC) may result in loss of containment, and/or uncontrolled gas flow. This may lead to minor impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage. (P50)	28	
385495	Electric Operations	Fossil Protection and Control Systems	Unintended operation or non-operation of powerhouse protection, DCS and SCADA systems may result in public and employee safety and reliability issues.	27	
258414	General Counsel	Inaccurate Legal Advice	The risk of inaccurate legal advice may result in adverse judgments, penalties or fines, investigations and enforcement actions, contract claims, and damage to reputation and credibility.	27	
258424	General Counsel	Misrepresentations in Front of Courts or Agencies	Misrepresentations in front of courts or agencies may result in sanctions, penalties and fines, investigations and enforcement actions, stricken pleadings, issue preclusion, loss of attorney-client privilege, and damage to reputation and credibility.	27	
251937	Gas Operations	CCE002 - Other Outside Force - Third Party Damage - Vehicles	Third party damage due to vehicles on a meter which should have meter protection may result in loss of containment and ignition leading to public safety issue.	25	
251741	Gas Operations	CCE006 - Material or Weld - Poor Quality Control of Regulator/Meter Set Manufacturing	Poor quality control of regulator and meter set manufacturing may result in faulty equipment with loss of containment and ignition leading to public safety issue.	25	
251878	Gas Operations	CP004- Weather Related/Outside Forces - Flooding (System Safety)	The risk of failure of the levees at McDonald Island protecting compression or storage assets may result in flooding.	25	
252868	Electric Operations	Distribution Overhead Streetlight Structures	Streetlight structural failure or bulb/lamp burnout may result in safety issues or property damage.	25	
250457	Finance	F and R Compliance Performance Risk	Systemic non-compliance within F&R resulting from not having an effective compliance program and ethical culture.	25	
387909	Gas Operations	LNG030.1 - Incorrect Station Ops	Risk of engineering or human operations errors that may cause major safety impacts on personnel or the public.	25	
387709	Gas Operations	CCE028 - Other Outside Force - Grounding	Unsafe grounding configuration on the houseline at the meter location may result in a potential ignition of gas during maintenance activities resulting in a safety impact employees.	24	
318209	Gas Operations	CP023 - Kettleman Station compressor outtage due to any cause (System Safety)	The risk of outage at Kettleman Station due to any cause on CWD may result in loss of service	24	
318065	Gas Operations	CP026 - Tionesta Station compressor outtage due to any cause (System Safety)	The risk of outage at Tionesta Station due to any cause on CWD may result in loss of service	24	
318190	Gas Operations	CP027 - Burney Station compressor outtage due to any cause (System Safety)	The risk of outage at Burney Station due to any cause on CWD may result in loss of service	24	
318197	Gas Operations	CP028 - Gerber Station compressor outtage due to any cause	The risk of outage at Gerber Station due to any cause on CWD may result in loss of service	24	
390661	Gas Operations	CP033 - Topock Station compressor outtage due to any cause	The risk of outage at Topock Station due to any cause on CWD may result in loss of service	24	
252788	Electric Operations	Distribution Overhead Line Equipment – Protective	Failure of distribution overhead protective line equipment may result in public or employee safety issues, fire, or property damage	24	
298587	Gas Operations	LNG022 - Incorrect Operations - CNG Quick Change Bottle Safety	Risk of mishandling of quick change bottles may result in vessel damage, significant loss of containment, fire and/or explosion that could cause severe major safety impacts to personnel in close proximity.	24	
385579	Electric Operations	Fossil Balance of Plant	Failure of or interaction with plant systems may result in employee safety issues, environmental damage, and reliability issues.	23	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
390194	Gas Operations	GSO006 - Market Liquidity Risk	The risk of reduced liquidity in at risk products brought on by fewer trading counterparties may result in reduced revenues to PG&E.	23	
390206	Gas Operations	GSO008 - Demand Risk	The risk of low customer demand may result in lower throughput and ultimately reduced revenue.	23	
385476	Electric Operations	Hydro Balance of Plant	Failure of or interaction with plant systems may result in employee safety issues, environmental damage, and reliability issues.	23	
298572	Gas Operations	LNG019.1 - Third-Party Damage - CNG Tube Trailer Parked (Reliability)	Risk of collision of a vehicle or other object with CNG Tube Trailer (Portable Supply Equipment parked) or other incident may result in vessel damage, and significant loss of containment, fire and/or explosion that could cause reliability impacts.	23	
252057	Gas Operations	MC024 - Equipment Related - LoS Complex Station	The risk of an under-pressure event at complex station due to equipment failure may result in loss of supply and downstream pressure cycles.	22	
390784	Gas Operations	MC027 - Equipment Related - Terminal/Large Complex	The risk of an underpressure event at a terminal or large complex station caused by equipment failiure may result in loss of service impact to multiple customer locations	22	
390799	Gas Operations	MC035 - Equipment Related - Backbone (PLS) Stations	The risk of an underpressure event at a complex station (backbone / PLS stations) caused by equipment failure may result in loss of service impact to multiple customer locations	22	
317413	Gas Operations	STO030.1-1st, 2nd, 3rd Party - All Segments	Leak or pipeline or mechanical damage to storage assets due to 1st, 2nd, and 3rd Party equipment/vehicles who may not have followed work procedures that may result in uncontrolled flow of gas, outages or replacement of gas supply. This may lead to minor impact on public or employee safety, outages or replacement of gas supply, property damage and/or minor environmental damage. (P50)	22	
251557	Human Resources	Compliance Performance Risk	Failure to have an effective compliance program and ethical culture in Human Resources may result in reputation loss, erosion of employee trust, and financial/legal penalties against PG&E	20	
251204	Nuclear Generation	Liquid Waste Transportation Incident	An incident associated with liquid waste transportation may result in an inadvertent release of a significant amount of radioactive or industrial material to the environment, which could lead to public and employee safety issues, adverse publicity, and unknown financial impacts.	20	
251736	Gas Operations	STO024 - Weather & Outside Forces - McDonald Island	McDonald Island levee break that may result in loss of well, reservoir or facility isolation and access, and uncontrolled flow. This may lead to significant impact on prolonged outages or replacement of supply, property damage, and/or environmental damage.	20	
251711	Gas Operations	DMS002 - Excavation Damage Third Party, No Rupture (P50)	Damage to gas distribution facilities from a third party may result in damage to pipe, but no loss of containment. (P50)	19	
252848	Electric Operations	Distribution Overhead Transformers	Failure of or contact with energized distribution transformers may result in public or employee safety issues, fire, or property damage.	18	EDOH6
252873	Electric Operations	Distribution Overhead Line Equipment – Voltage Regulators, Boosters, and Capacitors	Failure of, or interaction with distribution overhead voltage line equipment may result in public or employee safety issues, fire, oil spill, or property damage.	18	EDOH7
318010	Gas Operations	CP017 - Equipment Related - Deferred maintenance	The risk of deferred preventive or corrective work on equipment (excludes compliance work) may result in potential safety impacts and loss of service.	18	
390666	Gas Operations	CP030 - Incorrect Operations	The risk of incorrect operation of critical compression or storage processing equipment may result in reduced transmission capacity or storage withdrawal capacity on CWD and causing core customer outage	18	
333155	Gas Operations	DMS041 - Incorrect Operations - Fusion Joints (P50)	Failure of a fusion joint may result in significant customer outage impacts and loss of containment, but no ignition (P50)	18	
387220	Safety and Shared Services	Hazardous Substance Mechanism	Discontinuation of the ability to use the Hazardous Substance Mechanism (HSM), or a change in the allocation of recovery for remediation costs for approved sites could result in increased costs to the business.	18	
385659	Electric Operations	Fuel Cell Systems	Failure of or interaction with fuel cell systems may result in public or employee safety issues or significant property damage.	18	
385427	Electric Operations	Photovoltaic Systems	Failure of or interaction with solar panels or inverters may result in public or employee safety issue.	18	
252863	Electric Operations	Substation Grounding Systems	Ineffective substation grounding system design, construction, or maintenance may result in employee and public safety issues and equipment damage.	18	
320376	Human Resources	HR Business Partners and Labor Relations	The risk of employee unrest, work stoppage or failure to follow regulatory or plan design requirements may result in fines or penalties.	17	
251461	Customer Care	Integrity of Payment Processing	The risk of interruption of Customer Care's ability to issue bills and/or process payments due to facility unavailability may result in negative reputational ipact, decreased customer satisfaction and trust, or significantly-delayed or unrealized revenue.	17	
317418	Gas Operations	STO017.1-External Corrosion-Pipeline	Leak on the pipeline due to external corrosion which may result in the loss of pipeline isolation and access as well as an uncontrolled flow or lost production. This may lead to minor impact on public or employee safety, prolonged outages or net replacement of supply, property damages and/or environmental damage. (P50)	17	
391082	Gas Operations	STO033 - Disposal Well - Gill Ranch	Failure to dispose of produced fluids in a Gill Ranch disposal well which may result in the curtailment of gas production.	17	
391088	Gas Operations	STO034 - Internal/External Corrosion - Disposal-Well - Gill Ranch	Failure of casing integrity due to corrosion may result in the loss of Gill Ranch disposal well isolation, curtailment of gas production, and/or environmental damage.	17	
385301	Safety and Shared Services	Environmental (Manufactured Gas Plant [MGP] sites Remediation)	Failure to adequately manage PG&E's relationships with stakeholders (communities and the media), associated with the remediation of historical Manufactured Gas Plants (MGPs) locations could result in increased remediation costs, perceived public health concerns, regulatory fines and/or reputational damage.	16	
250447	Finance	Inappropriate release of data	The inappropriate release of employee or vendor data could expose the Company to significant regulatory, or legal action, and negative media coverage.	15	
320381	Human Resources	Compensation Program	The risk of paying employees unfairly, or inability to produce records of fair pay practices may result in: -Legal or regulatory non-compliance -Fines, penalties or increased costs -Reduced employee engagement	14	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
318215	Gas Operations	CP023.1- Kettleman Station Outage due to Power Outage	The risk of Kettleman station outage due to power outage may result in a loss of service.	14	
304074	Gas Operations	DMS012 - Material or Weld - Mechanical Fittings	Failure of mechanical fittings (2" Metfit installed between 1999 and 2006) susceptible to corrosion of outer ring may result in loss of containment but not gas migration or ignition.	14	
317647	Gas Operations	GSO004 - Loss of Supply from Interconnected Pipelines and Third Party Storage	The risk of reliance on pipeline interconnects and third party storage could result in incorrect supply and uncontrolled customer outages and or emergency curtailments of non core cutomers (including power plants).	14	
317635	Gas Operations	GSO005 - Portfolio Management Risk	The risk of changes in firm capacity ratings may result in over selling firm capacity and impact customer satisfaction and revenue opportunities.	14	
317627	Gas Operations	GSO011 - Inadequate Visibility into the Pressures and Flows on the Networks	The risk of having inadequate visability into the pressures and flows on pipeline networks could result in potential customer outages, unknown over or under pressure events and inability to identify equipment performance.	14	
385462	Electric Operations	Hydro Material Release into Water	Equipment failure could lead to release of materials into nearby bodies of water, causing adverse environmental conditions, unknown financial impacts, and reputation damage.	13	
298562	Gas Operations	LNG017.1 - Third-Party Damage - LNG Tanker Parked (Reliability)	Risk of collision of a vehicle or other object with LNG Tanker (Portable Supply Equipment parked) may result in tank rupture, significant loss of containment, fire and/or explosion that could cause severe reliability impacts.	13	
259139	Corporate Affairs	Risk of Noncompliance	Failure to apply an effective system of controls to mitigate issues related to company policies, lobbying, gifting (political and charitable) and ex parte within the Corporate Affairs organization.	13	
251972	Gas Operations	DMS003 - External Corrosion on Steel Piping	External corrosion on steel piping may result in loss of containment, but no gas migration or ignition.	12	
318912	General Counsel	Cybersecurity	An intentional/unintentional loss of control of information and systems used for gas and electric operations (e.g., SCADA, plant networks, trading, etc.) and business operations (e.g., finance, human resources, back office, etc.) may result in: life safety events; operational reliability impacts; privacy and intellectual property theft; and revenue and reputation loss.	11	
389547	Gas Operations	DMS049 - Material or Weld - Isolation Valve failure	MAOP Isolation valve failures between transmission pressure and distribution pressure systems may result in an over-pressurization event.	11	
384316	Safety and Shared Services	Emergency Response	The risk of failure to perform Logistics functions within the Incident Command System (ICS) due to lack of proficient resources for establishing and managing the EOC, Base Camps, and Staging Areas in a full activation incident associated with PG&E's restoration efforts could result in business impacts such as an extended response effort and increased costs	11	
387603	Finance	Regulatory Accounting Error	Risk of regulatory accounting error due to misinterpretation of regulatory decision, failure to follow regulatory accounting guidance, or inaccurate or incomplete data. Potential consequences include re-statements of financial statements filed with the SEC and FERC, regulatory penalties or disallowances, misguided business decisions, and loss of goodwill at the CPUC or FERC.	11	
317429	Gas Operations	STO005.1-Corrosion-Well Casing	Leak in well casing pipe due to corrosion which may result in the minor loss of well isolation and access, uncontrolled flow of gas and loss of production which may result in minor impact on public or employee safety, outages or net replacement of supply, property damages and/or minor environmental damage. (P50)	11	
303924	Gas Operations	CCE023 - Natural Forces -Settlement of Soil	Settlement of soil causing riser to break meter or regulator piping to multi-residental buildings may result in loss of containment ignition and public safety issue.	10	
251957	Gas Operations	DMS011 - Incorrect Operatons - Regulator (Semi-High or High Pressure)	Regulator station fails to control pressure to semi-high or high pressure distribution system may result in overpressure on distribution system piping leading to multiple hazardous leaks leading to public safety issues.	10	
304116	Gas Operations	DMS025 - Material and Weld - Curb Valves	Lack of seal on curb valves may result in loss of containment, with no migration or ignition.	10	
298552	Gas Operations	LNG014 - Third-Party Damage - Fuel Theft	Risk of fuel theft from the Dispenser (Fueling Station) or under collection accounts could result in loss of revenue.	10	
252037	Gas Operations	MC020 - Equipment Related - LoS Complex/Simple Station	The risk of an under-pressure event at complex/simple station due to equipment failure may result in loss of supply to a large customer facility.	10	
251843	Gas Operations	STO001- Third Party Damage - Reservoir	A 3rd party drilling into a storage field if PG&E does not have the rights/licenses or has lease payment lapse to store gas in all of the acreage which may result in a loss of gas and PG&E trespass. This may lead to replacement of gas supply and property damage.	10	
303898	Gas Operations	CCE016 - Other Outside Force - Inoperable or Inaccessible Service Valve	Inoperable or inaccessible service valve on multi-residental building may result in delayed emergency response leading to extended gas release, ignition and public safety issue.	9	
332470	Customer Care	Inability to Meet Program Goals or Performance Metrics	The risk of PG&E's inability to meet goals or performance metrics associated with third-party programs may result in negative reputational impact, loss of revenue, and potential loss of programs.	9	
258429	General Counsel	Risk of Noncompliance	Risk of Noncompliance can result in: Systemic failure to comply with regulatory, legislative, or legal requirements resulting in fines, legal proceedings, reputational damage	9	
251967	Gas Operations	DMS007 - Natural Forces - Cast Iron Material	Cast iron material or joint failure may result in significant customer outage impacts and loss of containment with ignition leading to public safety issues.	8	
390200	Gas Operations	GSO007 - Price Risk	The risk of a long-term flat price curve may result in reduced revenue.	8	
251932	Gas Operations	CCE001 - Incorrect Operations	Failure to replace customer meters may result in over billing on multiple accounts leading to non-compliance with CPUC requirements and impact to reputation or, may result in under billing on multiple accounts leading to financial loss to PG&E.	7	
303904	Gas Operations	CCE021 - Other Outside Force - Fire	Fire adjacent to assets that could destroy meter or regulator set may result in gas release leading to increased fire damage.	7	
389541	Gas Operations	DMS048 - Internal Corrosion - Mainline Drips	Mainline drips not maintained may result in internal corrosion creating loss of containment and possible migration	7	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
250422	Finance	Paying Incorrect Taxes	The company could either underpay estimated taxes and be subject to penalties, or overpay taxes, and lose the time value of the cash and incur costs to get the funds refunded to us.	7	
390825	Gas Operations	MC005 - Incorrect Operations - Backbone (PLS) Stations	The risk of an underpressure event at a complex station (backbone / PLS stations) caused by incorrect operations may result in loss of service impact to multiple customer locations	6	
390818	Gas Operations	MC008 - Incorrect Operation - Terminal/Large Complex	The risk of an underpressure event at a terminal or large complex station caused by incorrect operations may result in loss of service impact to multiple customer locations	6	
251706	Gas Operations	TRA002 - External Corrosion (P50)	Leak in transmission pipeline due to external corrosion may result in loss of containment and/or uncontrolled gas flow that can lead to minor impact on public safety, minor property damage, brief/no outages and/or minor environmental damage. (P50)	6	
251777	Gas Operations	TRA007 - Third Party / Mechanical Damage (P50)	Leak in transmission pipe resulting from mechanical damage by a 3rd party may result in loss of containment and/or uncontrolled gas flow that can lead to impact on public safety, minor property damage, brief/no outages. (P50)	6	
318490	Corporate Affairs	Employee Qualifications	The risk of having a workforce where employees do not meet qualifications may result in safety issues, reputational damage, re-work and could lead to legal action against the company.	5	
251997	Gas Operations	MC011 - Incorrect Operations - LoS Complex/Simple Station	The risk of an underpressure event at a complex/simple stations caused by incorrect operations may result in loss of service impacting multiple customer locations	5	
250442	Finance	Financial Statement Misstatement	Risk of material error to the financial statements, requiring restatement of earnings with the applicable regulatory agency.	4	
298547	Gas Operations	LNG013 - Third-Party Damage - Dispenser Vandalism	Risk of Dispenser (Fueling Station) failure caused by vandalism may result in dispenser outage and pressure/shrapnel that could cause moderate safety impacts to nearby personnel.	4	
298577	Gas Operations	LNG020 - Third-Party Damage - CNG Bottle Trlr Transpo Incident	Risk of vehicular incident (e.g., driver failure or unable to avoid, or third party action or equipment failure) may result in collisions or other incidents, and possibly loss of containment and/or other severe safety impact.	4	
251942	Gas Operations	CCE003 - Other Outside Force - Vandalism	Vandalism on meter set assembly may result in release of gas and ignition leading to public safety issue.	3	
304098	Gas Operations	DMS017 - Atmospheric Corrosion	Atmospheric corrosion on above ground facilities (e.g. risers, exposed spans), may result in loss of containment, but no ignition.	3	
250452	Finance	Fraudulent Payments - Accounts Payable	The occurrence of fraudulent payments could result in significant financial exposure to the company as well as regulatory or legal actions.	3	
387618	Finance	Inappropriate release of financial data	Inappropriate release of financial data could expose the Company to legal action, negative media coverage, adverse regulatory outcomes, and/or impact investor and public perception.	3	
312953	Gas Operations	TRA015 - Internal Corrosion (P50)	Leak in transmission pipeline due to internal corrosion may result in the uncontrolled flow of gas that can lead to minor impact on public or employee safety, minor/no outages, property damages. (P50)	3	
251962	Gas Operations	DMS006 - Material or Weld - T-caps	Plastic T-caps material failure may result in loss of containment, but no gas migration or ignition.	2	
258419	General Counsel	Missed or Late Filings	The risk of missed or late filings may result in default judgments, lost claims, penalties or fines, investigations, loss of good standing or qualification to conduct business, and damage to reputation and credibility.	2	
318538	Information Technology	Records Management	The risk of not implementing an effective records management program may result in the failure to construct, operate and maintain a utility system safely and prudently. For non-asset departments, the risk of not implementing an effective records management program may result in the failure of business processes that meet legal and regulatory compliance obligations.	2	
318922	General Counsel	Records Management (General Counsel)	Not implementing fully an effective records management program may result in the failure to construct, operate or maintain a safe system. For non-asset departments, not implementing fully an effective records management program may result in inadequate business processes. At the enterprise-level, there is an expectation that the company improve its overall information and records management program.	2	
251767	Gas Operations	TRA005 - Manufacturing Related Defects (P50)	Leak at longitudinal weld of transmission pipe may result in loss of containment and/or uncontrolled gas flow that can lead to negligible impact on public safety and negligible property damage. (P50)	2	
251340	Regulatory Affairs	Company Compliance Performance - Regulatory Affairs	Risk Systemic non-compliance resulting from not having an effective compliance program .	1	
355300	Safety and Shared Services	Compliance Performance Risk	A systematic failure in Safety & Shared Services Compliance program may lead to regulatory fines, civil and criminal prosecutions, sanctions, operational delays, public and employee injury or loss of life, reputational damage and lowered reliability. Score is based on DOT & Regulatory Compliance Score, which is highest residual score for S&SS.	1	
298582	Gas Operations	LNG021 - Third-Party Damage - CNG Bottle Trlr Parked Collision (Safety)	Risk of collision of a vehicle or other object with CNG Bottle Trailer or CNG module (Portable Supply Equipment parked) may result in vessel damage, significant loss of containment, fire and/or explosion that could cause minor safety impacts.	1	
391130	Gas Operations	STO035 - Outside Forces (Geological) - Reservoir	Geological uncertainty which may result in the loss of inventory or gas migration from the storage reservoir or influx of reservoir fluids impounding or trapping storage gas.	1	
401268	Gas Operations	CCE035 - Natural Forces - Lightning Strike	Lightning strike causing damage to the meter set with release of gas and ignition that can lead to impact on safety and property damage.	0	
390656	Gas Operations	CP031 - Bethany Station compressor outtage due to any cause	The risk of outage at Bethany Station due to any cause on CWD may result in loss of service	0	
400113	Gas Operations	DMS055 - Other Outside Force - Grounding	Electric distribution grounding in the vicinity of distribution piping may result in a potential ignition of gas during maintenance activities resulting in a safety impact employees	0	
400118	Gas Operations	DMS056 - Natural Froces - Lightning Strike	Lightning strike causing damage to the distribution pipe with release of gas and ignition that can lead to impact on public and employee safety, outages and property damage.	0	

Risk Profile ID	Risk LOB	Risk Name	Risk Description	Risk Score	EO Risk Designation
318917	General Counsel	Employee Qualifications	The risk of employees working without meeting legally required qualifications.	0	
390352	Gas Operations	GSO012 - Gas Control Operator Error	An error made by a gas control operator may lead to...	0	
390363	Gas Operations	GSO013 - SCADA Outage	Failure of the Gas Operations SCADA System may lead to...	0	
390377	Gas Operations	GSO014 - Physical Security - Gas Control Center Attack	A physical security attach against the Gas Operations Control Center may lead to...	0	
390387	Gas Operations	GSO015 - GOC System Failure Effecting Field Coordination and Response	Failure of Gas Operations Control systems that enable field coordination and response may lead to...	0	
278772	Safety and Shared Services	Life Safety Management	Failure to maintain proper life safety procedures and resources could lead to injury or loss of life of employees and the public, as well as regulatory fines and sanctions.	105	
391560	Safety and Shared Services	Motor Vehicle Safety	TBD	0	
391487	Customer Care	Natural Gas Appliance Testing (NGAT) Inspections	Risk Description: Risk of improper gas and carbon monoxide assessments before or after measure installation may result in unsafe carbon monoxide exposure and/or unmitigated gas leaks.	36	
388313	Safety and Shared Services	Supply Chain Fraud – Violations of Code of Conduct	Violations of the PG&E employee code of conduct, Sourcing code of conduct and Supplier Code of conduct could lead to actual or attempted fraud potentially resulting in impacts to regulatory compliance, loss of trust and financial impacts.	0	