Application: 17-04-010
(U 39 E)
Exhibit No.:
Date: December 8, 2017
Witness(es): Various

PACIFIC GAS AND ELECTRIC COMPANY

APPLICATION FOR A CERTIFICATE OF PUBLIC CONVENIENCE AND NECESSITY TO OPERATE AS A COMPETITIVE LOCAL EXCHANGE CARRIER

REBUTTAL TESTIMONY

PACIFIC GAS AND ELECTRIC COMPANY
APPLICATION FOR A CERTIFICATE OF PUBLIC CONVENIENCE
AND NECESSITY TO OPERATE AS A
COMPETITIVE LOCAL EXCHANGE CARRIER
REBUTTAL TESTIMONY

TABLE OF CONTENTS

PACIFIC GAS AND ELECTRIC COMPANY

CHAPTER 1

REBUTTAL TESTIMONY ON

POLICY ISSUES

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 1
REBUTTAL TESTIMONY ON
POLICY ISSUES

TABLE OF CONTENTS

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 1
REBUTTAL TESTIMONY ON
POLICY ISSUES

A. Introduction

Q 1 Please state your name and the purpose of this rebuttal testimony.

A 1 My name is Aaron August. This testimony responds to policy issues raised in the direct testimony of the Office of Ratepayer Advocates (ORA),[1] The Utility Reform Network (TURN),[2] and the California Association of Competitive Telecommunications Companies (CALTEL).[3]

Q 2 Does Pacific Gas and Electric Company (PG&E or the Company) have general concerns with the parties' testimony?

A 2 Yes, PG&E has three general concerns that I will address in this testimony:

1) ORA's recommendations place limitations and conditions on PG&E's proposed Competitive Local Exchange Carrier (CLEC) that are inappropriate as they would prevent competition and ratepayer benefits, and in some cases conflict with existing requirements under the California Public Utilities Commission (Commission) General Orders;
2) TURN and CALTEL recommendations to deny PG&E's application incorrectly focus on requiring PG&E to have a detailed business plan, instead of PG&E's overall goal to promote competition and benefit ratepayers (and incent shareholders) from shared revenues; and
3) TURN's recommendation that PG&E's proposed after tax (net) revenue sharing methodology be rejected and that a before tax (gross) revenue sharing methodology be adopted would result in fewer, if any, ratepayer benefits because PG&E will not invest in projects that do not appropriately compensate shareholders for their risk.

B. Summary of Parties' Positions

Q 3 What are the parties' positions?

---

1 ORA Testimony of S. Hunter, Testimony of A. Clark, Testimony of C. Reed.

2 TURN Testimony of R. Finkelstein.

3 CALTEL Testimony of S. DeYoung.

A 3 ORA recommendations include items related to financial processes and controls[4]; revenue sharing[5]; and continuation of existing dark fiber services.[6] ORA also recommends imposing additional conditions, restrictions and requirements[7,8] that are not appropriate.

TURN recommends that PG&E's application be denied[9] or that PG&E be required to submit supplemental testimony before approval,[10] and that, if approved, a before-tax (gross) revenue sharing methodology be implemented.[11]

CALTEL recommends that PG&E's application be denied, or that PG&E be required to submit supplemental testimony before moving forward with consideration of approval of PG&E's application.[12]

Q 4 What is PG&E's position relative to parties' proposed recommendations?

A 4 Despite parties' positions, PG&E's application for a Certificate of Public Convenience and Necessity (CPCN) should be granted. Allowing a new facilities-based company to enter the telecommunications market will enhance competition in the public interest. PG&E's existing large network, already deployed to support the Company's gas and electric operations, will enable the timely and efficient deployment of new service offerings at competitive prices. PG&E's proposed revenue sharing mechanism would further benefit PG&E's end-use gas and electric customers by offsetting their rates, while appropriately compensating PG&E's shareholders for the risk they take on. In sum, PG&E's CPCN would result in benefits to many stakeholders (the public interest, through competition; telecommunications services customers, through potential new offerings at competitive prices; PG&E's gas and electric customers, through reduced rates; and PG&E's

---

4 ORA Testimony of S. Hunter, p. II-1, lines 5-6.

5 ORA Testimony of S. Hunter, p. II-1, lines 3-4.

6 ORA Testimony of A. Clark, p. 3, lines 1-5.

7 ORA Testimony of A. Clark, p. 2, line 18 through p. 3, line 18.

8 ORA Testimony of C. Reed, p. 8, lines 13-28.

9 TURN, p. 2, lines 3-6.

10 TURN, p. 4, lines 15-17.

11 TURN, p. 6, line 9; p. 7, line 22.

12 CALTEL, p. 14.

shareholders, through earnings to compensate them for the risk of funding this business) and enhance the strength of the telecommunications services market in California. Imposing additional restrictions on PG&E's CLEC business or existing non-tariffed products and services as a condition of granting a CPCN, or imposing a revenue sharing methodology that does not appropriately compensate shareholders for their risk, could inhibit the viability of a CLEC business and therefore limit or prevent the many benefits that could result from PG&E operating as a CLEC.

I address PG&E's general position in some detail below, and I and other witnesses will address more specific issues in following chapters.

C. PG&E's Overall Reaction to Intervenors' Positions

1. ORA's Recommendations

Q 5 What is your response to ORA?

A 5 PG&E agrees with ORA's position on financial processes and controls, and partially agrees with ORA's approach to net revenue sharing (addressed in detail in Chapter 3 rebuttal testimony). PG&E disagrees with ORA on positions related to additional recommendations that impose conditions on PG&E that do not apply to other CLECs as these unfairly place PG&E at a competitive disadvantage and provide no incentive for PG&E to pursue the CLEC business. These issues are addressed in detail in rebuttal testimony Chapters 2, 3, 4 and 5.

2. TURN's Recommendations

Q 6 What is your response to TURN?

A 6 PG&E disagrees with TURN's recommendation to deny PG&E's application, as this will prevent ratepayers from benefitting from reduced rates through revenue sharing, and it would go against the Commission's goal to encourage additional entrants into the communications industry. PG&E also disagrees with TURN's proposed before tax (gross) revenue sharing mechanism, as this will result in fewer successful transactions because only the highest margin projects would appropriately compensate shareholders as explained further in rebuttal testimony Chapter 3. Thus, a loss of potential benefit to ratepayers would also occur in the form of reduced rates from shared revenues.

3. CALTEL's Recommendations

Q 7 What is your response to CALTEL?

A 7 PG&E disagrees with the recommendation of CALTEL to deny PG&E's application for the same reasons stated in A6 above. Additionally, PG&E disagrees with the suggestion that additional testimony is required because PG&E's initial application addressed the statutory and regulatory requirements related to granting a CPCN, and PG&E direct testimony addressed the issues raised in the Scoping Memo. PG&E addresses these issues in greater detail in subsequent chapters of rebuttal testimony.

D. Conclusion

Q 8 Please summarize your position.

A 8 PG&E's application for a CPCN to provide: (1) full facilities-based and resold competitive local exchange service throughout the service territories of AT&T California, Frontier California Inc., Consolidated Communications of California Company, and Citizens Telecommunications Company of California; and (2) full facilities-based and resold non-dominant interexchange services on a statewide basis, and PG&E's proposed revenue sharing mechanism, should be approved.

Q 9 Does this conclude your rebuttal testimony on policy issues?

A 9 Yes, it does.

PACIFIC GAS AND ELECTRIC COMPANY

CHAPTER 2

REBUTTAL TESTIMONY ON

BUSINESS PLAN ISSUES

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 2
REBUTTAL TESTIMONY ON
BUSINESS PLAN ISSUES

TABLE OF CONTENTS

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 2
REBUTTAL TESTIMONY ON
BUSINESS PLAN ISSUES

A. Introduction

Q 1 Please state your name and the purpose of this rebuttal testimony.

A 1 My name is Aaron August. This testimony responds to all or portions of the direct testimony of the Office of Ratepayer Advocates (ORA),[1] The Utility Reform Network (TURN),[2] and the California Association of Telecommunications Companies (CALTEL).[3]

B. Pacific Gas and Electric Company's Response to Intervenors' Positions

1. ORA

Q 2 What is ORA's position with regard to fiber lines installed in the power zone?

A 2 ORA recommends that Pacific Gas and Electric Company (PG&E) be prohibited from using "existing fiber lines installed in the power zone of utility poles for its CLEC operations and leases of dark fiber…"[4] and that PG&E be prohibited "from installing any additional fiber in the power zone for its Competitive Local Exchange Carrier (CLEC) operation and leases of dark fiber to other providers."[5]

Q 3 How does PG&E respond?

A 3 PG&E agrees with ORA's position with respect to the use of dark fiber installed in the power zone for CLEC operations.

Q 4 What is ORA's position with regard to PG&E's current dark fiber services?

A 4 ORA recommends that PG&E be required "to continue to offer its dark fiber services located in the communications space, as they are available today. PG&E should continue to make available, at a minimum, the same number

---

1 ORA Testimony of A. Clark, pp. 1-14.

2 TURN Testimony of R. Finkelstein, pp. 1-13.

3 CALTEL Testimony of S. DeYoung, pp. 4-14.

4 ORA Testimony of A. Clark, p. 2, lines 18-20.

5 ORA Testimony of A. Clark, p. 2, lines 21-22.

of fiber strands, and along the same routes, as currently offered to third parties as dark fiber or via fiber swaps."[6]

Q 5 How does PG&E respond?

A 5 PG&E does not agree with ORA's position. PG&E does not agree that a Certificate of Public Convenience and Necessity (CPCN) should be conditioned on new requirements relating to its existing products and services. PG&E offers these leases and swaps under contract terms negotiated by two independent parties, when the benefits of such agreements represent the best value to PG&E's ratepayers. If benefits for PG&E ratepayers no longer exist, PG&E would cease to offer such leases and swaps. PG&E does not currently anticipate changes to existing agreements covering dark fiber and that it does not currently plan changes to its current dark fiber service offerings.[7] In any case where a dark fiber agreement is covered by a license agreement subject to General Order 69C, it is necessary that the license is revocable, and if strands are required for PG&E gas or electric operations, the strands must be reclaimed for utility use.

Q 6 What conditions does ORA recommend with regards to PG&E future customer agreements for fiber services?

A 6 ORA recommends that PG&E CLEC operations be prohibited "from entering into exclusive arrangements with any single customer utilizing PG&E's existing fiber network and generally maintain the ability to serve multiple customers."[8] Additionally, ORA recommends that PG&E be prohibited "from leasing every fiber strand along any route of its existing network to a single customer."[9]

Q 7 How does PG&E respond?

A 7 PG&E does not agree with ORA's position. Imposing these restrictions would limit PG&E's ability to fairly compete with other CLECs who don't have to meet these requirements. Additionally, it would not always be

---

6 ORA Testimony of A. Clark, p. 3, lines 1-5.

7 CLEC_DR_TURN 001-Q16.

8 ORA Testimony of A. Clark, p. 3, lines 1-5.

9 ORA Testimony of A. Clark, p. 3, lines 9-10.

possible to license or lease all available fiber strands along any segment to more than one customer. For example, where only two strands of fiber are available on a given route, and since most telecom equipment requires a strand for the transmit port and a separate strand for the receive port, it would not be possible to lease these strands to more than one customer. The adoption of this restriction would not be beneficial for the competitive market and could inhibit using the existing excess capacity to generate value for PG&E's ratepayers.

Q 8 What is ORA's position with respect to CLEC services offered by PG&E?

A 8 ORA recommends that the specific services PG&E's CLEC is allowed to offer be identified in Ordering Paragraphs.[10]

Q 9 What is PG&E's response?

A 9 PG&E disagrees with ORA's position. PG&E has stated its intent to offer "lit fiber" and other services that are requested by potential communication service customers. Placing limitations on a PG&E CLEC operation that are not imposed on other CLEC service providers inhibits competition, and ultimately will provide less benefit to PG&E ratepayers through shared revenues and less benefit to communication customers of all service providers by limiting competition.

Q 10 What is ORA's position with respect to PG&E's ability to offer retail CLEC services to residential customers?

A 10 ORA recommends that PG&E be required to file an application to seek authority if it desires to offer retail communication services to residential customers in the future.[11]

Q 11 What is PG&E's response?

A 11 PG&E agrees with ORA's position. PG&E is not requesting authority to provide retail communication services to residential customers.

Q 12 Does ORA make additional recommendations?

---

10 ORA Testimony of A. Clark, p. 3, lines 13-14.

11 ORA Testimony of A. Clark, p. 3, lines 15-18.

A 12 Yes. ORA recommends that PG&E should be required to establish uniform rates for its services.[12]

Q 13 How does PG&E respond?

A 13 PG&E disagrees with ORA's recommendation. By offering services on a non-tariffed basis, PG&E and its customers will retain the benefit of clearly defined terms through individually negotiated agreements, but have the added advantage of being able to execute agreements to meet individual customers' unique needs. This allows for a more targeted approval process for each modification, allowing PG&E to begin the work necessary to provide services more quickly.[13]

2. TURN

Q 14 What recommendation does TURN make?

A 14 TURN recommends that PG&E present supplemental testimony that more fully discusses the third-party assessment it obtained for purposes of developing its CLEC application.[14]

Q 15 What is PG&E's response?

A 15 PG&E disagrees with TURN's position. PG&E did not rely solely on the assumptions in the consultant study, but rather used the information generated as part of its internal assessment in evaluating its approach to entering the CLEC business. Use of a consultant study to provide support for a view that opportunities for a competitive offering are available, and entrance into the communication business could benefit ratepayers and shareholders, is a prudent step in making a business decision. A requirement for supplemental testimony regarding the third party assessment, the product of which PG&E has provided to TURN, is not warranted.

3. TURN and CALTEL

Q 16 Do parties make other recommendations?

---

12 ORA Testimony of A. Clark, p. 11, lines 11 through p. 12, line 3.

13 PG&E Testimony, p. 2-6, line 26 through p. 2-7, line 13.

14 TURN Testimony of R. Finkelstein, p. 4, lines 15-17.

A 16 Yes, TURN and CALTEL recommend that PG&E's application for a CPCN should be denied due to a failure to meet the requirements for a CPCN.[15] CALTEL presents that PG&E "did not provide any additional information explaining how PG&E meets the basic statutory requirements imposed on all CLECs…to obtain a CPCN" and criticizes PG&E for the lack of a detailed business plan.[16] Similarly, TURN presents that PG&E's proposed "stage-gate" approach to the proposed CLEC business is not appropriate and effectively places PG&E in the position of requesting "the equivalent of an advisory opinion from the Commission."[17]

Q 17 What is PG&E's response?

A 17 PG&E disagrees with this recommendation. CALTEL incorrectly states that PG&E failed to provide requisite information in its Application and in its testimony. It is my understanding that the Application included the information required pursuant to Decision 13-05-035. CALTEL's statement is misleading in that it does not consider that PG&E's initial Application (A.17-04-010) is an existing part of the record in this case and that as included in Sections C, D, E, and R in the Application PG&E has provided the information necessary to show that it meets requirements.[18] For example, PG&E provided estimated customer counts for years 1 and 5 and it provided a general description of the services it may provide upon the Commission granting the Application.

4. CALTEL

Q 18 Does CALTEL raise other issues?

A 18 Yes. CALTEL also opines that PG&E testimony contradicts previous statements regarding discussions or negotiations with potential customers of its proposed CLEC.[19]

Q 19 How does PG&E respond?

---

15 TURN Testimony of R. Finkelstein, p. 2, line 4 through p. 4, line 20; CALTEL Testimony of S. DeYoung, pp. 4-14.

16 CALTEL Testimony of S. DeYoung, pp. 4 and 8-10.

17 TURN Testimony of R. Finkelstein, p. 3, line 2.

18 PG&E Testimony, pp. 2-11, lines 8-13.

19 CALTEL Testimony of S. DeYoung, p. 4.

A 19 CALTEL is incorrect. In direct testimony, PG&E indicates that it works closely with telecommunication companies in providing existing Non-Tariffed Products and Services (NTP&S).[20] PG&E points out many times, however, that it has not engaged in direct discussions or negotiations related to providing specific CLEC services with any customer.[21] Simply being aware of inquiries related to service that might be provided by a CLEC, but is not offered as an existing NTP&S by PG&E (in the course of ongoing interactions as PG&E provides existing NTP&S to communication customers) does not constitute an active discussion or negotiation related to provision of CLEC services.

Both CALTEL and TURN seem to suggest that all CPCN applicants have been required to submit a detailed business plan and that PG&E should be required to do the same.[22] While I am not a lawyer, I am not aware of a Commission or statutory requirement directing applicants seeking a CPCN for purposes of providing telecommunications services to provide a detailed business plan. In addition, my understanding of the application for a CPCN is to request approval from the Commission to pursue the CLEC business, which does not seem to be an advisory opinion.

C. Conclusion

Q 20 Please summarize your position.

A 20 PG&E has satisfied the requirements and PG&E's Application (A.17-04-010) for a CPCN to provide: (1) full facilities-based and resold competitive local exchange service throughout the service territories of American Telephone and Telegraph, Inc. California, Frontier California Inc., Consolidated Communications of California Company, and Citizens Telecommunications Company of California; and (2) full facilities-based and resold non-dominant interexchange services on a statewide basis should be granted.

Q 21 Does this conclude your rebuttal testimony?

A 21 Yes, it does.

---

[20] PG&E Testimony, p. 2-3, line 22 through p. 2-4, line 5.

[21] PG&E Testimony, p. 2-4, lines 28-30, is one example.

[22] CALTEL Testimony of S. DeYoung, pp. 8-11; TURN Testimony of R. Finkelstein, p. 2, line 8 through p. 4, line 20.

PACIFIC GAS AND ELECTRIC COMPANY

CHAPTER 3

REBUTTAL TESTIMONY ON

REVENUE SHARING

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 3
REBUTTAL TESTIMONY ON
REVENUE SHARING

TABLE OF CONTENTS

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 3
REBUTTAL TESTIMONY ON
REVENUE SHARING

A. Introduction

Q 1 Please state your name and the purpose of this rebuttal testimony.

A 1 My name is Richard Patterson. This testimony responds to the direct testimony of the Office of Ratepayer Advocates (ORA),[1] and The Utility Reform Network (TURN)[2] that address Pacific Gas and Electric Company's (PG&E) revenue sharing proposal.

Q 2 Does PG&E have concerns with the parties' testimony?

A 2 Yes, PG&E's principal concern is that the revenue sharing mechanisms, proposed by TURN and ORA, would result in few, if any, profitable Competitive Local Exchange Carrier (CLEC) investments. Adoption of their proposals would likely result in PG&E not pursuing a CLEC business, and little, if any, of the excess capacity on PG&E's fiber system being used to benefit Utility ratepayers and the customers of California's telecommunications industry.

B. Summary of Parties' Positions

Q 3 What are the parties' positions?

A 3 TURN proposes that CLEC revenues be shared between Utility ratepayers and shareholders with 70 percent of the gross revenues going to Utility ratepayers.[3] TURN also suggests that it may be preferable for PG&E to organize its CLEC business as an affiliate, and have that affiliate contract with the Utility for the use of the Utility's fiber network.[4]

ORA accepts PG&E's proposed after-tax net revenue sharing mechanism, but recommends that the sharing proportions be set at

---

1 ORA Testimony of S. Hunter.

2 TURN Testimony of R. Finkelstein.

3 TURN, p. 12, line 25, and lines 9-11.

4 TURN, p. 5.

75 percent ratepayer and 25 percent shareholder, rather than PG&E's proposed 50-50 sharing mechanism.[5]

Q 4 What is PG&E's position, relative to parties' proposed recommendations?

A 4 PG&E's proposed revenue sharing mechanism provides a fair and reasonable benefit to ratepayers, while leaving enough profit potential as an incentive for PG&E to develop and operate a CLEC business. On the other hand, the adoption of the recommendations of ORA or TURN would result in substantially fewer, if any, ratepayer benefits. The California Public Utilities Commission (CPUC or Commission) should approve PG&E's proposed revenue sharing mechanism, rather than these recommendations, for the reasons explained in more detail below.

C. PG&E's Response to Intervenors' Positions

1. TURN

Q 5 TURN offers a number of arguments that support its revenue sharing proposal. Do any of those arguments have merit?

A 5 No. As I will show below, TURN's arguments do not adequately support their recommendation.

Q 6 In your direct testimony you provide illustrative, or possible, gross and net revenue estimates. Please describe how those net revenue estimates would be impacted by TURN's proposal to allocate 70 percent of the gross revenue to ratepayers.

A 6 Table 3-1 below shows the estimated gross and net revenue as shown in my direct testimony, and as adjusted to reflect TURN's 70 percent sharing proposal.

TABLE 3-1
(MILLIONS OF DOLLARS)

Line No.		Year 1	Year 2	Year 3	Year 4	Year 5
1	Gross Revenue	–	1	4	12	23
2	Net Revenue (PG&E proposal)	(2)	(3)	(3)	1	7
3	Net Revenue (TURN proposal)	(2)	(4)	(6)	(7)	(9)

[5] ORA, p. III-2, lines 1-5.

Net revenues are just pre-tax profits, which means that the after-tax net revenue, i.e., profit, under TURN's proposal would be negative, and hence would result in earnings losses in each of the five years.[6] Extending the table to 20 years would show negative net revenue in each year.[7] PG&E would not enter the CLEC business with expected net losses such as these. TURN's 70 percent gross revenue sharing proposal should be rejected because it will result in no benefits.

Q 7 What percentage of gross revenue would work from PG&E's perspective?

A 7 PG&E opposes a gross revenue sharing mechanism, for the reasons explained in PG&E's direct testimony.[8] There is no reasonable way, without experience in the CLEC business, to determine the percentage of gross revenue that would: (1) result in an adequate opportunity for PG&E to make investments in a CLEC business and still earn a fair return on those investments; and (2) result in a CLEC business that has enough scale economies to make a viable business and compete with other CLECs. This is why PG&E proposed after-tax net revenue (profit) sharing—it does not rely on having to determine the right amount of a gross revenue share needed to generate enough income for a viable business. Although PG&E also does not, and cannot know, the exact percentage of net revenue sharing that would optimize ratepayer benefits, 50 percent sharing seems reasonable in the face of uncertainty, and given that by using PG&E's excess fiber capacity PG&E should be able to generate profit sufficient to share and also earn the cost of capital on its CLEC investments.

Q 8 TURN suggests the Commission should ignore PG&E's claim that the CLEC business is a low margin business. Do you agree?

A 8 No. It is important to understand the relationship between gross revenue and costs, as explained in PG&E's direct testimony.[9] In short, the profit margin is an important driver in determining an adequate revenue sharing

---

6 Including tax impacts would reduce the loss by the amount of the tax benefit in each year, but after-tax profits would still all be negative.

7 The data for this table is taken from a 2015 consultant report that contains seven years of forecast revenue and cost estimates. PG&E extrapolated that data to 20 years.

8 PG&E Direct Testimony, pp. 3-2 to 3-4.

9 *Id*, p. 3-2, lines 22-27.

mechanism. To illustrate, assume the 7 percent average pre-tax net margin, shown in Attachment A of my direct testimony, for eight telecommunications companies is equal to that needed to just compensate those companies for their cost of capital. In that event, a revenue decrease of 10 percent, or a cost increase of 10 percent, would wipe out all, or almost all, profits. On the other hand, if an adequate pre-tax profit margin were 60 percent, then a 10 percent decrease in revenue, or a 10 percent increase in costs, would result in a 10-15 percent drop in profits, which means the choice of sharing percentage is much less critical to the success of the business. To the extent that PG&E's CLEC business ends up being a low, or relatively-low, margin business, similar to the telecommunications companies in PG&E's sample, then the selection of a sharing percentage for a gross revenue method becomes highly critical to the success of the business. The Commission should not ignore the margin data from these telecommunications companies, and should use this information as a major reason to reject a gross revenue sharing mechanism.

Q 9 TURN claims that PG&E's analysis of the net margins of other California CLECs are not adequately comparable to the margins that might be experienced by PG&E's CLEC business. Do you agree?

A 9 No. The eight companies analyzed by PG&E have average, pre-tax margins that range from a negative 6 percent to a positive 18 percent, and have a range of operations and cost structures. Although PG&E's cost structure would reflect the benefit of PG&E's existing fiber network, PG&E's cost structure may also reflect costs significantly higher than the CLECs analyzed, and may well be within the range of the companies analyzed. PG&E believes the number of companies analyzed is large enough to provide a reasonable mean and variance of the net margin that PG&E may realize.

Q 10 TURN asserts that PG&E's analysis of net margins of other California CLECs is contradicted by data from PG&E's existing telecommunications related services. Do you agree?

A 10 No. TURN supports its argument with data provided by PG&E, and claims that this data shows the gross margin from PG&E's existing dark fiber-related Non-Tariffed Products and Services (NTP&S) to range from

64-97 percent.[10] This is not a relevant data point, since PG&E will incur startup and other costs, and must make incremental investments to acquire and own additional equipment in order to provide CLEC services. This is a critical difference, since the revenues generated by the CLEC business must be adequate, after taxes and sharing, to compensate PG&E for those costs, including the cost of capital. Factoring in those costs would substantially reduce the margins.

Additionally, directly comparing PG&E's proposed CLEC to Southern California Edison Company's (SCE) CLEC business would not be a good benchmark without knowing SCE's cost structure and investment criteria. For example, SCE may be constrained by its sharing mechanism to investments that have high net margins.

A benchmark TURN omitted from its testimony, but was included in the data it received for PG&E's telecommunications related NTP&S (of which dark fiber is a subset) is the pre-tax net margin for all of PG&E's telecommunications related NTP&S. That data shows a pre-tax net margin ranging from 38-48 percent. However, these margins reflect NTP&S activities that have no incremental investment costs, and hence are likely to be much higher than the margins that PG&E's CLEC business may experience, given the necessary incremental investment costs.

TURN's argument to ignore the evidence of margins from other telecommunications companies, and that PG&E's CLEC business may also be relatively low margin, should be disregarded.[11]

---

10 It appears that the data PG&E provided to TURN was shown in a format that could be easily misinterpreted. As a result, the margins computed by TURN from PG&E's data incorrectly included negative revenues as expenses, which substantially impacts the calculation of the percent margin. Recalculating the margins with negative expenses included in revenue shows the margin ranges from 59-75 percent for dark fiber licenses and use of conduit for placement of cable NTP&S.

11 TURN also (TURN, p. 10, lines 1-11) misapplies the concept of net vs. gross margin when TURN argues that it is the benefits per opportunity that matter, not the maximization of profit that would occur under PG&E's proposal. The level of sharing that would optimize benefits for ratepayers and/or telecom customers cannot be known or predicted without being able to precisely predict all the future revenues and costs. It is not a function of the number of opportunities but of the long-term profitability of those opportunities.

Q 11 Assuming that the right percentage of gross revenue to share could be determined, do you agree with TURN's claim that a gross revenue sharing mechanism is far simpler and easier to understand and administer, and reduces the likelihood of disputes about the reasonableness of the CLEC's incremental costs?[12]

A 11 No. TURN overstates the complexity of net vs. gross revenue sharing. Net revenue sharing is currently used in PG&E's non-tariffed mover services, and PG&E is unaware of any complaints that the net sharing mechanism is too difficult to understand or administer. All the parties to Utility rate proceedings deal with far more complex financial and rate issues, and the simple calculations for net sharing are easily understood and implemented. Further, there is no basis for TURN's assertion that a gross sharing mechanism would reduce the likelihood of disputes about the reasonableness of the CLEC's incremental costs. Incremental costs would still have to be tracked in order to ensure separation of those costs recovered in the General Rate Case (GRC). A gross sharing mechanism does not ensure that incremental costs would not be scrutinized for reasonableness and avoid disputes.[13]

Q 12 TURN claims a net revenue sharing mechanism creates a counterintuitive cost recording incentive.[14] Do you agree?

A 12 No. TURN's claim supposes that PG&E would falsely classify Utility costs as CLEC costs, in order to have the CLEC revenue serve as the recovery mechanism for the Utility costs. However, the same argument applies to TURN's gross revenue sharing proposal, since PG&E could falsely classify CLEC revenue as gas or electric revenue. TURN's argument would not support any sharing mechanism, is based on an assumption that PG&E will act in bad faith, and has no merit.

---

12 TURN, p. 9, lines 15-16.

13 Intervenors in Utility GRCs can and do scrutinize such costs through the discovery process, and often propose changes to the amounts and methods for estimating or classifying those costs. All of the CLEC's costs will be subject to the same process as other costs.

14 TURN, p. 10, Section 5.3.1.

Q 13 TURN's 70/30 ratepayer/shareholder pre-tax gross revenue sharing mechanism appears to be based on the assumption that PG&E can provide CLEC services with just dark fiber.[15] Is that assumption correct?

A 13 No. As explained in PG&E's application and testimony, PG&E's CLEC would have to incur marketing and other business development costs, as well as incremental capital investments, to use its fiber in a CLEC business and provide telecommunications services. Yet TURN's example in its testimony[16] assumes there are no such costs, hence appearing to justify the 70 percent allocation of gross revenue to Utility ratepayers. TURN's revenue sharing proposal is based on the incorrect assumption that PG&E will incur very little cost to operate a CLEC, and should be rejected.

Q 14 TURN cites a CPUC decision for Sempra Utilities, in which a 75/25 ratepayer/shareholder revenue allocation for San Diego Gas & Electric Company's (SDG&E) research and development (R&D) activities was adopted,[17] and a 50/50 net revenue sharing mechanism for new NTP&S was rejected. Are these decisions relevant for PG&E's CLEC?

A 14 No. Neither of the examples is relevant in this proceeding. The 75/25 ratepayer/shareholder mechanism applied to royalties received from SDG&E's R&D investments, which are fully funded by ratepayers, and SDG&E shareholders bear no risk. This treatment is different than PG&E's CLEC business, where shareholders would fully fund the incremental investments, and bear all the risk. The decision's rejection of a 50/50 sharing mechanism may have been appropriate if customers were bearing up to half the costs. However, unlike the situation described by TURN, shareholders will fund all the costs, and bear all the risk with PG&E's CLEC business.

Q 15 TURN claims PG&E's approach to the review of CLEC costs is inadequate.[18] Do you agree?

---

15 TURN, p. 12, lines 11-14.

16 TURN, p. 12, lines 15-19.

17 TURN, p. 9, lines 3-6.

18 TURN, p. 11, lines 25-27.

A 15 No. TURN and other intervenors would be able, through discovery, and typically in PG&E's GRCs, to review both recorded and forecast incremental CLEC costs, just as they have the same opportunity to review all other costs of PG&E's operations, both recorded and forecast, that are considered in PG&E's GRCs.

Q 16 Please explain why TURN's suggestion that it may be preferable for PG&E to organize its CLEC business as an affiliate is adverse to the benefit of Utility ratepayers.

A 16 One of PG&E's primary objectives in establishing its CLEC business is to provide benefits to its gas and electric customers through a revenue sharing mechanism.[19] If PG&E were to establish a CLEC business in an affiliate, then PG&E would not propose a revenue sharing mechanism. Instead, Utility ratepayers would realize benefits from the revenues that the Utility would receive from the CLEC for use of excess capacity on the Utility's fiber network and for use of other Utility resources, such as Information Technology personnel. While this business structure may be able to provide a material portion of the benefits achievable under PG&E's proposed structure, it would also have much higher transaction costs, since the "transactions" that would have occurred within the Utility would now occur between two corporate entities where such transactions are governed by contracts. Higher transaction costs occur because the CLEC would incur legal and operating costs to put contracts in place, modify them, administer them, and renew them. Resources acquired through contracts would create inefficiencies that would be avoided by having the CLEC be a line of business within the Utility. For example, contracts that specify the type of work to be done for the CLEC, and specifications for which Utility employees might provide that work, may be ambiguous in some circumstances, resulting in the CLEC spending resources to clarify the contract, work out a letter of understanding, or perhaps source certain services from third parties. Further, operating a CLEC affiliate could require additional attention from senior management, which is also counter to the objectives of the New Revenue Development Department. The CLEC may find that without the

---

19 PG&E Prepared Testimony, p. 1-2, lines 6-7.

operating flexibility that comes from being within the Utility, the CLEC would not fully use excess capacity within the Utility, thus defeating the goal of using excess Utility resources for the benefit of Utility ratepayers. Hence, the overall result of using an affiliate structure for a CLEC would be less revenue to offset the costs of the Utility's gas and electric operations.

2. ORA

Q 17 Please explain why you disagree with ORA's revenue sharing proposal.

A 17 As explained above, PG&E's primary objective for its CLEC business is to leverage Utility assets for the benefit of its Utility ratepayers. Revenue sharing, whether gross or net, is a cost of that business, and the higher that cost the lower the return PG&E would earn on its incremental capital investments in the CLEC business. ORA's proposal to share 75 percent of the profits with ratepayers would substantially increase the cost of the CLEC business, and leave PG&E with little or no return on its incremental CLEC capital investments. To the extent that PG&E is presented with CLEC investment opportunities, but could not expect to earn its cost of capital on those investments as a result of the higher cost of sharing, then PG&E will not make those investments, and ratepayers will then forego the benefits they would have obtained.

Q 18 Would ORA's proposed change from a 50 percent net sharing rate to 75 percent make that much of a difference?

A 18 Yes. To illustrate, assume the CLEC business needs to earn, after sharing, a 10 percent return on its equity invested in the business. At 50 percent sharing PG&E would need to earn a 20 percent pre-sharing return in order to be left with the needed 10 percent. But at 75 percent sharing, PG&E would need to earn a pre-sharing return of about 40 percent to be left with a 10 percent return for PG&E's investors. A 40 percent return is likely to be very challenging, and result in many fewer investments, and hence substantially lower benefits for customers. Using the revenue and cost estimates that were used to derive Table 3-1, the estimated 20-year return on the incremental capital needed to generate those revenues is about 25 percent, a return adequate for 50 percent sharing—given the uncertainty in estimating such amounts—but nowhere close enough for 75 percent profit sharing.

Q 19 ORA also justifies its 75 percent sharing proposal with the assertion that ratepayers fund the facilities that are in place to facilitate PG&E's CLEC business.[20] Do you agree?

A 19 No. Customers pay for Utility gas and electric service and bear some of the risk of Utility operations, however, they will not pay for any of the incremental capital or expense needed by PG&E to operate its CLEC business, and will assume no additional risk as a result of the CLEC business. In addition, the risk of recovering those costs is entirely borne by PG&E's shareholders. Given these circumstances, and the objectives to generate benefits for ratepayers, and for PG&E to have an adequate opportunity to earn a fair return on its invested capital, PG&E believes that its proposed 50/50 net sharing mechanism is reasonable and can meet those objectives.

D. Conclusion

Q 20 Please summarize your position.

A 20 ORA and TURN have both proposed revenue sharing mechanisms that would result in substantially less benefits for ratepayers, and possibly none at all. PG&E's excess fiber capacity is a valuable asset that can be used to benefit not just Utility ratepayers but also the California telecommunications industry and its customers. To use this excess capacity requires PG&E to make incremental investments, as well as to incur other costs to develop and run the CLEC business. PG&E must have the opportunity to earn a reasonable return on its investments to compensate its shareholders for the additional risk they bear, and the proposals of ORA and TURN do not do that. PG&E recommends the Commission adopt PG&E's proposal without modification.

Q 21 Does this conclude your rebuttal testimony?

A 21 Yes, it does.

---

[20] ORA, p. III-2, lines 11-13.

PACIFIC GAS AND ELECTRIC COMPANY

CHAPTER 4

REBUTTAL TESTIMONY ON

PG&E'S RIGHT-OF-WAY PROCEDURES

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 4
REBUTTAL TESTIMONY ON
PG&E'S RIGHT-OF-WAY PROCEDURES

TABLE OF CONTENTS

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 4
REBUTTAL TESTIMONY ON
PG&E'S RIGHT-OF-WAY PROCEDURES

A. Introduction

Q 1 Please state your name and the purpose of this rebuttal testimony.

A 1 My name is Karen Khamou. This testimony responds to the direct testimony of The California Association of Telecommunications Companies (CALTEL),[1] and the Office of Ratepayer Advocates (ORA).[2]

Q 2 Does Pacific Gas and Electric Company (PG&E) have concerns with the parties' testimony?

A 2 Yes, PG&E has the following specific concerns that I will address in this testimony:

1. CALTEL does not acknowledge the connection between PG&E's detailed explanation of right-of-way access procedures as a means to effectively facilitate and ensure nondiscriminatory access.
2. CALTEL asserts that right-of-way access process changes are necessary if the Certificate of Public Convenience and Necessity (CPCN) is approved.
3. ORA's recommendation of a mandated 45-day review timeframe for all access applications disregards safety-related considerations.

B. Summary of Parties' Positions

Q 3 What are the parties' positions?

A 3 CALTEL's position is that PG&E's testimony concerning nondiscriminatory access was inadequate, mainly because it did not include process changes CALTEL presumes are necessary by virtue of PG&E's anticipated Competitive Local Exchange Carrier (CLEC) status.[3]

ORA's position is that PG&E should be held to the 45-day application review timeframe currently imposed for Incumbent Local Exchange Carriers

---

1 CALTEL Testimony of Sarah DeYoung.

2 ORA Testimony of Adam Clark.

3 CALTEL Testimony of Sarah DeYoung, p. 5.

(ILECs), reasoning that this timeframe would incentivize PG&E to review applications without discrimination in the event it is approved to operate as a CLEC.[4]

Q 4 What is PG&E's position relative to parties' proposed recommendation?

A 4 In sum, PG&E's existing right-of-way access procedures adequately ensure nondiscriminatory access, which PG&E further elaborates below. Regarding ORA's position, PG&E believes the 45-day response timeframe required of ILECs should not be imposed upon PG&E for safety reasons. I address PG&E's positions in more detail below.

C. PG&E's Overall Reaction to Intervenors' Positions

1. Process Changes Are Not Needed to Ensure Nondiscriminatory Access

Q 5 You state you disagree with CALTEL's claims that PG&E's testimony inadequately addressed necessary process changes to ensure nondiscriminatory access. Can you explain the basis for your concerns?

A 5 Yes. The wording of the scoping memo read as follows: "…testimony shall include…a description of what, *if any*, changes it plans to those [right-of-way access] procedures, terms, and conditions if a CPCN is granted [*emphasis added*]."[5] PG&E believes that existing processes adequately facilitate nondiscriminatory access and will continue to do so in the event PG&E is granted a CPCN.

In describing its current processes that facilitate right-of-way access, PG&E explained the criteria for receiving and processing an application for access, and emphasized by way of detailed steps how the processes, as they currently exist, facilitate and will continue to facilitate nondiscriminatory access.[6] Neither CALTEL nor any other intervenor has objected to any element of the right-of-way process described in PG&E's testimony, whether from the perspective of an existing CLEC or in anticipation of PG&E being a CLEC. CALTEL did not raise any concerns or allege that PG&E's existing

---

4 ORA Testimony of Adam Clark, p. 2.

5 Scoping Memo and Ruling of Assigned Commissioner and Administrative Law Judge Application (A.) 17-04-010 (Scoping Memo), p. 7, July 13, 2017.

6 A.17-04-010 PG&E's Prepared Testimony, Chapter 4.

process hinders nondiscriminatory access, yet it assumed that process changes were needed in order to provide nondiscriminatory access.

CALTEL did question why the Commercial Mobile Radio Service (CMRS) process was included in PG&E's Testimony.[7] This process was included because while it currently involves right-of-way wireless access granted to CMRS carriers, it may include CLECs in the future.[8] Although CLECs and CMRS carriers are two distinct entities, the process for any additional entities granted right-of-way wireless access may be similar to that of the CMRS carriers. The inclusion of the CMRS process in PG&E's testimony anticipated this possibility,[9] and in the event CLECs are granted wireless access as part of the order, PG&E will use the CMRS process as a benchmark to developing a wireless right-of-way access process for CLECs.

Having stated these concerns about CALTEL's testimony, I will elaborate on PG&E's methods for upholding nondiscriminatory access, including the first-come, first-served principle.[10]

Pre-Application Access to Information

Among the request for access application requirements, the ones relevant to pre-application access to information are PG&E facility maps and pole datasheets. These materials are currently provided in response to written request in accordance with General Order 95 Rule 44.4. However, PG&E is currently developing an online portal that will not require written requests.[11] Using this secure portal, CLECs and other approved entities will be able to query maps and pole data remotely and on demand.

Regarding access to customer information, the proposed PG&E CLEC unit will not have access to information concerning other entities' right-of-way access applications. The PG&E CLEC unit and the Joint Utilities Group would be two separate entities with separate and distinct

---

7 CALTEL Testimony of Sarah DeYoung, pp. 11-12.

8 D.16-01-046,*Decision Regarding the Applicability of The Commission's Right-of-Way Rules to Commercial Mobile Radio Service Carriers*, p. 139, Ordering Paragraph 6.ii.

9 To clarify a previous statement, this process is comparatively new but has received a significant number of applications.

10 D.98-10-058, Appendix A, Rule 6A.

11 Qualifying participants will need to execute a non-disclosure agreement with PG&E to access the online portal.

reporting structures. At no time will the PG&E CLEC unit be advised about or have access to customer-specific information pertaining to existing applications for specific infrastructure, except in the event of a denial to the PG&E CLEC unit due to an existing application for the same infrastructure. In this case, the PG&E CLEC unit will be advised only that the specific infrastructure has already been applied for and is unavailable for more attachments, in accordance with current practice.

Application Processing

When processing right-of-way access applications to solely-owned poles, PG&E complies with the nondiscrimination principle of first-come, first-served by using a date stamped application intake process. Applications are then routed for review in the order received, and application receipt dates, dates of approval/denial, and reasons for denial are available and auditable.[12] These elements would not change with the introduction of a PG&E CLEC unit.

Applications for tenancy on jointly owned poles are not submitted to PG&E. For jointly owned poles, all CLECs apply to the owner of the communication space, typically AT&T. PG&E expects to use the ownership process as defined in the Northern California Joint Pole Association Routine Handbook, which is available to the California Public Utilities Commission (CPUC).

2. The 45-Day Response Timeframe Imposed on ILECs Should Not Be Imposed on PG&E

Q 6 You state you disagree with ORA's proposal to impose a 45-day review timeframe on PG&E to incentivize PG&E to review applications in a nondiscriminatory manner. Can you elaborate?

A 6 Yes. PG&E supports timely access to infrastructure for CLECs, but PG&E believes safety is a more important consideration. Although PG&E was asked for data concerning reasons for application denial, a crucial piece it has not yet been asked about is: why do some applications take over 45 days to process, whether approved or denied? The answer is because PG&E is working in the interests of both safety and access. Requests for

---

12 See also ORA DR 004 Response.

access cannot be regarded solely as an access issue; rather, safety considerations may drive response times.

To elaborate, evaluation of an application includes a review of pole loading, including major elements used by third-party engineering to calculate the safety factor. PG&E takes a conservative approach when determining whether a submission meets the required safety factor, or when the pole loading calculations contain elements that are not in accordance with PG&E records; therefore, the responsible PG&E representative will contact the applicant or applicant's engineer to review and resolve the issues. If working with the submitting entity does not resolve the concerns—which often directly bear upon the safety factor—PG&E estimators may conduct a further review to ensure the required safety factor will be met for the proposed attachment. Working with the applicant and estimating takes time, as pole attachments often present unique situations.

Moreover, based on PG&E's understanding, the ILEC pole approval process is not as extensive as that of electric utilities. The suggestion that an electric utility should be held to ILEC timeframes should first consider whether the scope of the ILECs' application review processes necessitated by a mandated 45-day review period is sufficient for a thorough pole loading review.

Regardless of CLEC status, given PG&E's responsibility to appropriately manage pole load, PG&E must review proposed pole load of an internal unit with the same care as external to ensure safety. To do otherwise would effectively increase risks of pole failure. Because safety is critical, the imposition of a strict 45-day review period would only incentivize faster denial of applications if there is not enough time, which will likely cause CLECs to review and resubmit applications. I believe that ORA's proposed timeframe needs to be further examined to ensure it does not effectively

permit pole overloading, which is a broader policy endeavor that should be addressed in the other appropriate proceedings.[13]

Lastly, as part of the Scoping Memo, PG&E was asked to include information on mean and median response times to requests for access processing.[14] PG&E provided that information for the past two calendar years, the results of which were a mean of 37 days and a median of 25 days. As a follow-up, ORA requested a detailed breakdown of application response data which was provided on a customer, job-specific level.[15] The majority of applications were processed well within the 45-day timeframe.[16]

D. Conclusion

Q 7 Please summarize your position.

A 7 PG&E's existing right-of-way access processes provide sufficient controls to ensure nondiscriminatory treatment of all applications and can accommodate the addition of PG&E's CLEC business if the CPCN is approved. ORA's recommendation for the 45-day review timeframe is inappropriate in this proceeding and does not take into account safety concerns that must be addressed during the review period.

Q 8 Does this conclude your rebuttal testimony?

A 8 Yes, it does.

---

13 The Scoping Memo and Ruling of Assigned Commissioner and Administrative Law Judge A.17-04-010 (Scoping Memo), at p. 8, directed that broad policy issues should be addressed in other proceedings. I am aware that the Commission is considering whether there should be a uniform set of access rules in R.17-06-028 and I believe that ORA's proposal for a 45-day timeframe is more appropriate in that proceeding and the review in that proceeding will be in terms of applicability to all entities, not just PG&E.

14 Scoping Memo, p. 6, Item 2 b.

15 See ORA DR 004 Response.

16 See ORA DR 004 Response.

PACIFIC GAS AND ELECTRIC COMPANY

CHAPTER 5

REBUTTAL TESTIMONY ON

PG&E'S TELECOMMUNICATIONS NETWORK

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 5
REBUTTAL TESTIMONY ON
PG&E'S TELECOMMUNICATIONS NETWORK

TABLE OF CONTENTS

PACIFIC GAS AND ELECTRIC COMPANY
CHAPTER 5
REBUTTAL TESTIMONY ON
PG&E'S TELECOMMUNICATIONS NETWORK

A. Introduction

Q 1 Please state your name and the purpose of this rebuttal testimony.

A 1 My name is David Wright. This testimony responds to the direct testimony of the Office of Ratepayer Advocates (ORA).[1]

Q 2 Does Pacific Gas and Electric Company (PG&E or the Utility) have general concerns with ORA's testimony?

A 2 Yes, PG&E has three general concerns that I will address in this testimony:

1. ORA's request to have the Competitive Local Exchange Carrier (CLEC) data and PG&E Utility data in completely separate databases is not reasonable at all times, and places an undue burden for not sharing general information with specific utility platforms;
2. ORA's request to have a notification sent to ORA and the California Public Utilities Commission (CPUC or Commission) of any data breach within 24 hours, and a report within 10 days, may not be consistent with the applicable rules and reporting laws for a CLEC business; and
3. ORA's suggestion that adding the CLEC business will result in greater PG&E network vulnerability, or create increased operational risk, is not valid.

B. Summary of Parties' Positions

Q 3 What is ORA's position?

A 3 ORA's position is that all CLEC data should be separate from PG&E Utility data, not stored in the same databases.[2] ORA proposes a specific breach reporting cycle applicable to only PG&E.[3] ORA also suggests an increased

---

1 ORA Testimony of C. Reed.

2 ORA Testimony of C. Reed, p. 8, lines 18-20.

3 ORA Testimony of C. Reed, p. 8, lines 25-28.

operational risk to PG&E's networks by adding the CLEC business to the Utility portfolio.[4]

Q 4 What is PG&E's position relative to ORA's proposal?

A 4 PG&E believes that in some cases it is not feasible to have the CLEC and Utility data completely separated and that the CLEC data will need to be stored in shared Utility databases and systems. With regards to ORA's reporting requirement proposal, once PG&E becomes a CLEC, then PG&E's CLEC business unit will comply with all reporting rules and laws applicable to CLECs. Lastly, PG&E's existing standards and practices will be able to mitigate any potential increased cybersecurity risk. I address PG&E's general position in more detail below.

C. PG&E's Overall Reaction to Intervenors' Positions

1. It Is Unreasonable for PG&E to Store Utility Network and Infrastructure Data Separately, However, Confidential Customer Data Will Be Protected and Separate

Q 5 You state that ORA's position, which requires complete separation of CLEC and Utility data, is unreasonable and unfeasible. Please explain.

A 5 I disagree with ORA's proposal to not store CLEC data with Utility data in the same databases because there will be a few instances where some of the data will need to be comingled and cannot be separated. Certain telecommunications network maps and tables will need to be stored in shared databases with the Utility.[5] Specifically, PG&E Information Technology has a Graphical Information System (GIS) that stores and displays fiber cable information, down to the strand level. The GIS will store both CLEC and Utility data. For example, fiber strands in a PG&E cable, whether used by customers of the CLEC or the Utility, would be identified in the GIS tool. The name of the customer(s) will need to be captured as attribute data, and assigned to the fiber strand the customer resides on for the purposes of fiber cable relocations or restoration. However, confidential or private customer information or data, such as contract terms and

---

4 ORA Testimony of C. Reed, p. 9, lines 20-25.

5 See PG&E response, Answer 3b to ORA's DR_003_Q03.

transport services provided, would be protected and not stored in GIS or other shared databases.

2. PG&E Should Not Be Subject to Additional Requirements Not Imposed on Other CLECs

Q 6 What is ORA's proposed reporting requirement?

A 6 ORA proposes that PG&E's CLEC should notify the Commission, ORA, and the CPUC's Office of the Safety Advocate within 24 hours of a breach involving the CLEC network and provide a report and mitigation plan within 10 days.[6]

Q 7 Why do you disagree with ORA's reporting requirement proposal?

A 7 I disagree with ORA's proposal because it recommends a requirement that would only apply to PG&E's CLEC business and not any other CLECs. If granted the Certificate of Public Convenience and Necessity, PG&E's CLEC business unit will comply with all laws and requirements, including reporting requirements, applicable to all CLECs operating in California.

3. PG&E's Proposed CLEC Business Will Not Increase Overall Cybersecurity Risk

Q 8 What is ORA's position on PG&E's CLEC business and cybersecurity risks?

A 8 ORA's testimony asserts that PG&E's CLEC business will increase cybersecurity risk to PG&E's Utility Network.[7]

Q 9 You question the validity of ORA's position that PG&E's CLEC business increases cybersecurity risks. Please explain.

A 9 I disagree with ORA's suggestion that PG&E's cybersecurity risk will increase by adding the CLEC business, because PG&E existing standards and procedures for addressing cybersecurity risks will provide the necessary protections against threats. The primary reason I disagree is that the services offerings that the CLEC will provide do not expose PG&E assets that would typically be subject to cyber threats.

PG&E's 2017 Risk Assessment and Mitigation Phase (RAMP) testimony provides a detailed cybersecurity assessment for the following categories: Risk Assessment; Controls and Mitigations; Current Mitigation Plan

---

6 ORA Testimony of C. Reed, p. 8, lines 25-28.

7 ORA Testimony of C. Reed, p. 13, lines 20-22.

(2017-2019); and Proposed Mitigation Plan (2020-2022). In the event of a cybersecurity incident related to any of PG&E's business units, the RAMP testimony demonstrates that PG&E has a comprehensive plan in place to manage and mitigate cybersecurity risk as a whole.

Q 10 What is ORA's recommendation regarding the RAMP and 2017 General Rate Case (GRC) filing?

A 10 ORA recommends that PG&E provide a copy of the RAMP testimony (filed November 30, 2017) and provide additional comparison between the RAMP filing and the 2017 GRC submission related to threats and risks.[8]

Q 11 What is your response to ORA's recommendation?

A 11 I have provided the 2017 RAMP submission associated with cybersecurity as Attachment 1 to this chapter, as recommended by ORA. However, overall, I cannot speak to the RAMP and 2017 GRC filings, since I did not prepare the submissions in those proceedings. I anticipate that ORA's recommendations for descriptions of differences between the RAMP and 2017 GRC submissions, and certain metrics used, would be adequately addressed in the appropriate proceedings.

D. Conclusion

Q 12 Please summarize your position.

A 12 PG&E contends that ORA's positions regarding shared databases, reporting for breaches, and increased cybersecurity risk, are not reasonable. In some instances, PG&E Utility and high level CLEC data will need to be stored in the same databases, while confidentiality of the CLEC customer will be maintained. PG&E will comply with all appropriate CLEC reporting requirements, but disagrees with additional reporting requirements specific to PG&E's CLEC business. PG&E has internal processes in place to manage cybersecurity risk, and will use its expertise in the services offered to properly manage the CLEC network so it does not compromise the Utility networks.

Q 13 Does this conclude your rebuttal testimony?

A 13 Yes, it does.

---

8 ORA Testimony of C. Reed, p. 8, lines 2-8.

PACIFIC GAS AND ELECTRIC COMPANY

CHAPTER 5

ATTACHMENT 1

PG&E'S 2017 RISK ASSEMENT MITIGATION PHASE TESTIMONY

CHAPTER 18

CYBER ATTACK

PACIFIC GAS AND ELECTRIC COMPANY
2017 RISK ASSESSMENT MITIGATION PHASE
CHAPTER 18
CYBER ATTACK

PACIFIC GAS AND ELECTRIC COMPANY
2017 RISK ASSESSMENT MITIGATION PHASE
CHAPTER 18
CYBER ATTACK

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. Executive Summary

RISK NAME	Cyber Attack
IN SCOPE	A cyber attack that results in a loss of operational control or loss of company data (customer, employee, and/or business information)
OUT OF SCOPE	Nuclear, Diablo Canyon Power Plant (DCPP)[1]
DATA QUANTIFICATION SOURCES	Assessment informed by Pacific Gas and Electric Company (PG&E or the Company) data, Industry data (Verizon and Advisen), and subject matter expert (SME) judgment

Cyber-attack risk is a coordinated malicious attack purposefully targeting PG&E's core business functions, resulting in a loss of control of company information or systems used for gas, business, and electric operations.

The cyber-attack risk originates from adversaries that actively attempt to compromise PG&E systems for their own purposes. Attackers are constantly innovating, requiring PG&E to continuously adapt in order to defend against cyber attacks. Cyber-attack risk has been on PG&E's risk register since 2013. It is also an enterprise-level risk due to the potentially catastrophic consequences to safety and reliability of a successful cyber attack on PG&E's operational systems.

The following two core risk events are fundamental to cyber-attack risk for any utility, including PG&E:

1) Attacks on information technology with the objective of obtaining unauthorized access to data; and
2) Attacks on operational technology (OT) with the objective of disabling PG&E's ability to control the delivery of gas and electricity to our customers.

Both risk events generally result from four primary drivers that indicate potential deficiencies in a computing or operational environment:

- Governance – relates to executive leadership, framework management, policies, procedures, and roles and responsibilities;
- Business Process – includes risk assessments, controls and oversight;

[1] DCPP is not in scope for this risk. DCPP must comply with cyber security protocols that are aligned with the Nuclear Regulatory Commission's (NRC) Cyber Security Directorate.

- Systems and Infrastructure – encompasses protection of data storage and transfer, monitoring and diagnostics, and resolving obsolete or end-of-life technology; and
- People and Culture – includes awareness and training, employee engagement, and acquisition and development of specialized skillsets.

The core risk events and their associated drivers are addressed by existing controls and proposed mitigations. Controls and mitigations for the loss of operational control focus on preventing and reducing the impact of such events. The consequences of a loss of control event could include compromises to the integrity of operational assets, manipulation of those assets to cause malfunctions, degraded availability, and unplanned outages. Similarly, controls and mitigations for preventing and reducing the impact of data loss events are also deployed throughout the enterprise. The consequences of such events include the loss of the ability to ensure that sensitive information remains confidential, which in turn may lead to unauthorized access and theft of that information.

PG&E's controls and mitigations conform to programs aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF establishes the basic premises of an effective cybersecurity program. PG&E has adopted this framework to enable a standardized, objective approach for developing PG&E's programs to reduce cyber-attack risk.

Through the risk assessment undertaken as part of the Risk Assessment and Mitigation Phase (RAMP) process, PG&E confirmed the direction of its cybersecurity program in fulfilling its mission to deliver and maintain an integrated program to safeguard PG&E's digital assets. The modeling effort also reaffirmed PG&E's current understanding of risk drivers and consequences, as reflected in the mitigation programs for 2017-2019 and the proposed mitigation plan for the RAMP period of 2020-2022.

The next steps toward improving PG&E's understanding and analysis for cyber-attack risk include researching best practices on obtaining event data specific to OT systems and seeking better sources of information regarding data-loss risk. Industry agreement on the mapping of metrics to specific controls is another objective.

II. Risk Assessment

A. Background

The risks of cyber attack to PG&E's gas and electric distribution and transmission systems continue to increase. Cyber-attack incidents among all utilities have increased from a confirmed total of 3 in 2012 to 66 in 2015, the last year for which figures are publicly available. Along with the increase in incidents, threat intelligence indicates that cyber attacks have also become more ingenious and complex.

PG&E's cybersecurity program must protect against data security risks common to all companies, such as the risk of unauthorized disclosure of customer information. Additionally, PG&E must protect against risks to its operational systems that govern the flow of gas and electricity. Attacks on these systems could interrupt gas or electric service to PG&E's customers, and may potentially result in incidents that have catastrophic consequences, including injuries or deaths. As options for access and control become more complex, cybersecurity becomes more important for the overall safety of the PG&E operating environment.

PG&E's vision for cybersecurity takes the aforementioned factors into account. PG&E's goal is to have a cutting-edge program that employs the best professionals and leverages top-tier capabilities to safeguard its gas and electric system and protect sensitive information.

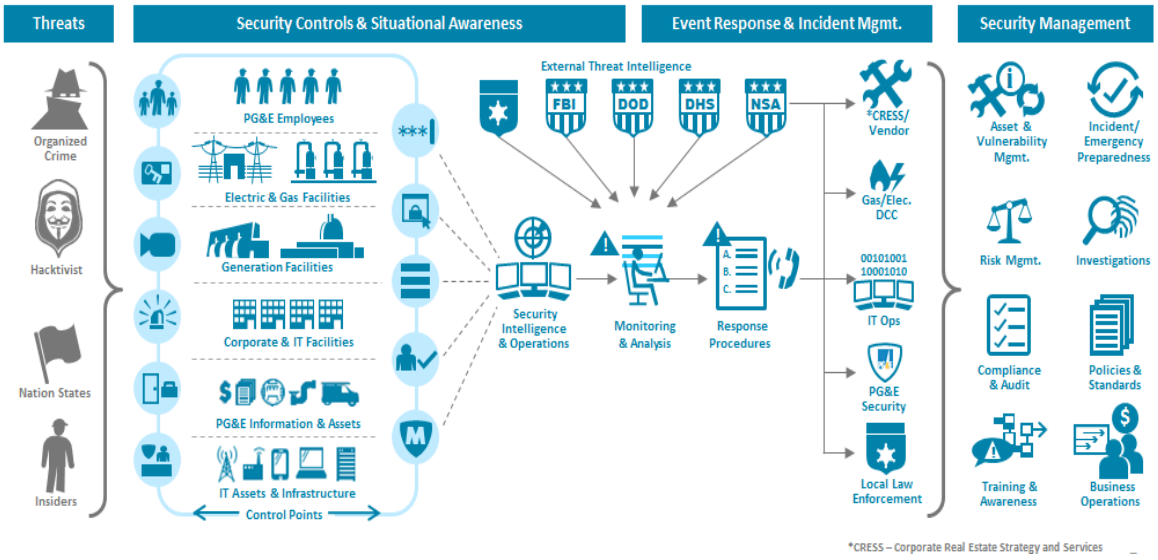
The mission of the PG&E cybersecurity organization is to deliver and maintain an integrated program that safeguards PG&E's digital assets by the following:

- Identifying our cyber-attack risks and defining mitigation strategies to ensure the safety of PG&E's customers, employees and contractors; and
- Building, deploying and operating effective security technologies and processes.

PG&E implements this vision through an increased focus on cyber-attack risk management, improved protective technologies, and insourcing its Cyber Security Intelligence and Operations Center (SIOC).

Figure 18-1 below illustrates the PG&E cybersecurity program's vision and mission. It indicates the source of threats, the assets that are targets for attacks, protective control points, and the role of the round-the-clock PG&E cybersecurity operations center which detects and combats attacks.

Figure 18-1: Security Strategy



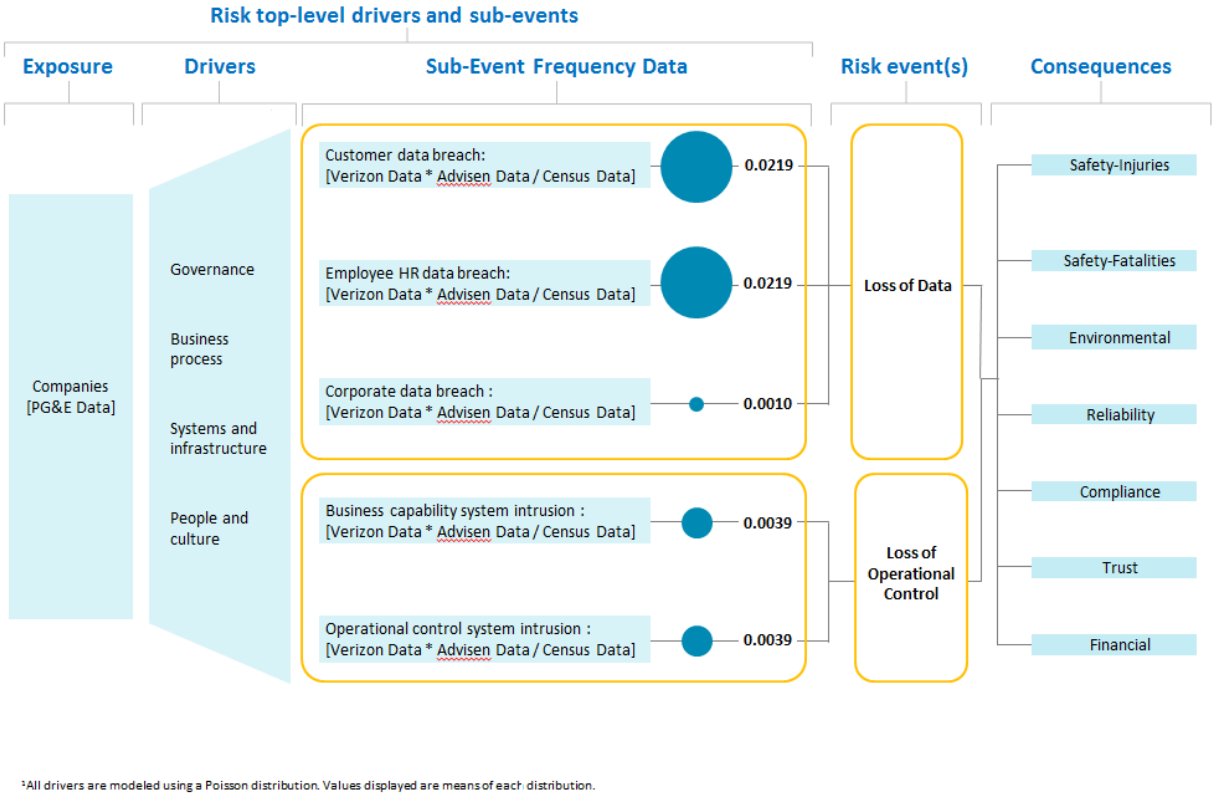
A cyber attack is a coordinated malicious attack that is purposefully targeted at PG&E's core business functions, resulting in a loss of control over information and systems used for gas, electric and business operations. Two categories of risk events are fundamental to cyber-attack risk:

- Attack on information technology with the aim of obtaining unauthorized access to data; and
- Attack on operational technology with the intent of crippling PG&E's ability to control the flow of gas and electricity to our customers.

When considering the safety impact of a cyber attack, the consequences of loss of control over operational technology are considered. Safety-related events stem primarily from a loss of operational control and not from data loss events. While there have been relatively few loss of control events in the industry, if an event occurred the consequences could have very high safety impacts. In addition to safety consequences, a successful cyber attack would also have impacts on system reliability, incur added costs to respond to a cyber attack, and cause loss of public trust in PG&E.

Figure 18-2 below is the visual representation of the risk bow tie which shows how inputs were represented in the risk model. Due to the unique nature of cyber-attack risk, the model looks at five sub-risk event types: customer data breach, employee data breach, corporate data breach, loss of operational control, and system intrusion. These five sub-risk event types are then grouped further to identify the Company's top two concerns: loss of data and a loss of operational control. This chapter speaks primarily to these two top concerns.

Figure 18-2: Risk Bow Tie



[1]All drivers are modeled using a Poisson distribution. Values displayed are means of each distribution.

B. Exposure

PG&E is exposed to potential cyber attack through its computer systems and networks. In the modeling effort, exposure was defined to be the Company in its entirety. This definition is necessary to compare to industry data reported on a per company basis. Within the Company, however, there are several likely points of potential intrusion such as the following:

- Computing systems or services accessible from untrusted networks. (Systems and Infrastructure)
- Computing systems or services owned or managed by third parties. (Business Process and People and Culture and Governance)
- Computing systems or services that are not maintained (for example, not being updated and/or using outdated operating systems). (Systems and Infrastructure)
- Malicious insiders (addressed more specifically through insider-threat risk). (People and Culture)
- Employees and contractors not engaging in good security practices. (People and Culture and Business Processes and Governance)

- The effectiveness of protective technologies such as firewalls, data loss prevention, anti-spam and anti-phishing filters, etc. (Systems and Infrastructure)

This is not an exhaustive list and exposure is hard to define. While the measurement of exposure is understood in a qualitative manner, it is difficult to quantify. For example, while counting the number of systems accessible from untrusted networks owned or managed by third parties or not maintained in a timely manner provides a rough notion of exposure, the fact remains that it only takes a vulnerability in one system to permit a cyber attack to happen. Moreover, protective technologies are designed to prevent attacks. It is not possible to measure attacks that don't occur. At best, it would be possible to measure indicators of cyber-attack attempts, but these would not be true cyber attacks. Analysis of the results of the bow tie analysis framework should take all the aforementioned factors into account.

C. Drivers and Associated Frequency

In modeling this risk, PG&E distilled the potential drivers of a cyber attack into four primary drivers. Due to the broad range and complexity of potential drivers to a cyber attack, these four categories consolidate all the drivers into their most fundamental level.

D1 – **Governance** – relates to executive leadership, framework management, policies, procedures, and roles and responsibilities. Poor governance could lead to a cyber attack through the lack of clear policies. For example, if the Company did not have a policy to disallow plugging in USB devices into the network this could introduce malicious software into PG&E's systems.

D2 – **Business Processes** – includes risk assessments, controls, oversight, and incident response. Business process could lead to a cyber attack through lack of controls or oversight. As an example, if the Company lacked a process to handle or identify vulnerabilities it could increase PG&E's exposure to a cyber attack.

D3 – **Systems and Infrastructure** – encompasses protection of data storage and transfer, monitoring and diagnostics, and resolving obsolete or end-of-life technology. Cyber attacks most often target individual systems directly. As a consequence, poorly maintained or outdated equipment can increase the exposure to a cyber attack.

D4 – **People and Culture** – includes awareness and training, employee engagement, and acquisition and development of specialist skillsets. Ultimately, people are the first line of defense for cyber attacks. Phishing emails are a common method of getting individuals to take actions that facilitate an attack.

A company culture of clicking email links without questioning the validity of the content or sender could increase the chance of a cyber attack.

As discussed in Sections III and IV, each of the risk drivers above are addressed by multiple mitigations.

While these drivers help to inform our mitigations, only the sub-risk events' relative frequency of events were used as inputs to the model due to constraints on available data. The data used in the model was comprised of Verizon and Advisen data on the frequency of cyber incidents among like size companies and used to inform our baseline risk. The Utility breaches from 2014, 2015 and 2016 in the Verizon Data Breach Investigation Reports[2] indicate yearly data breach frequencies range from 7 to 80 events per year and operational control breaches range from 0 to 7 events per year. The Advisen[3] loss data is used to estimate a compound annual growth rate of events and the percentage breakdown of data breach events into the various sub-risk events.

D. Consequences

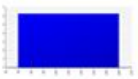
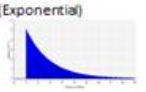
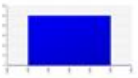
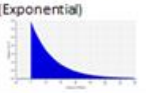
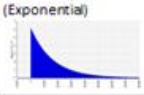
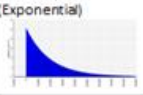
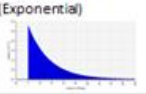
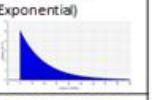
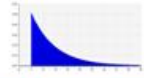
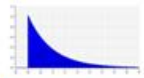
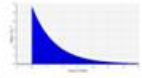
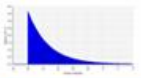
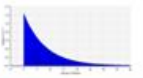
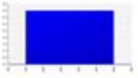
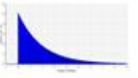
The range of consequences and the attributes that help describe the expected value and tail average risks and the associated multi-attribute risk score are shown below in Figure 18-3. The data available to establish consequence distributions for cyber attack risk are rare and generally unobtainable, therefore, for this risk, SME is used. Figure 18-3 shows that generally the 5th and 95th percentile values were given by the SMEs to describe the consequence impacts if a specific sub-risk event were to occur.

---

2 Verizon Data Breach Investigation Report: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016.

3 https://www.advisenltd.com/data/loss-data.

Figure 18-3: Consequence Attributes

	Safety-Injuries	Safety-Fatalities	Environmental	Reliability	Compliance	Trust	Financial
Source	SME Input	SME Input	SME Input	SME Input	SME Input	SME Input	SME Input
Customer data breach						Min:4%; Max:20% (Uniform) 	5%:$5M; 95%:$50M → Mean: $19.50M (Exponential) 
Employee HR data breach						Min:1%; Max:3% (Uniform) 	5%:$5M; 95%:$80M → Mean: $29.17M (Exponential) 
Corporate data breach			5%:$0; 95%:$50k → Mean: $16,110 (Exponential) 	5%:0; 95%:60k → Mean:19,332 (Exponential) 	N/A	Min:4%; Max:15% (Uniform) 	5%:$5M;95%:$100M → Mean: $35.61M (Exponential) 
Business capability system intrusion			N/A	N/A	N/A	Min:1%; Max:3% (Uniform) 	5%:$5M;95%:$50M → Mean: $19.50M (Exponential) 
Operational control system intrusion	5%:0; 95%:60 → Mean: 19.33 (Exponential) 	5%:0; 95%:3 → Mean: 0.97 (Exponential) 	5%:$0; 95%:$4.6M → Mean: $1.48M (Exponential) 	5%:0; 95%:840M → Mean: 270.65M (Exponential) 	5%:$70k; 95%:$25M → Mean: $8.10M (Exponential) 	Min:15%; Max:40% (Uniform) 	5%:$500k;95%:$5B → Mean: $1.95B (Exponential) 

	Safety-Injuries	Safety-Fatalities	Environmental	Reliability	Compliance	Trust	Financial
Outcome-TA-NU[1]	0.76	0.04	$61,580	11,507,908	$333,081	4.48%	$92,154,455
Outcome-TA-MARS[2]	0.21	1.04	0.01	28.77	0.03	22.40	55.29
						MARS Total	107.75

[1]Ave of Year 1-6 Tail Ave outcomes in Natural units
[2]Ave of Year 1-6 Tail Ave outcomes in MARS units

- **Safety – Injuries (SI):** Safety-related events stem exclusively from loss of operational control and not from data loss events. Events involving loss of operational control have been few in number, causing the data set for such events to be extremely small. Attackers may have incentives not to execute attacks that they otherwise could perform (for example, retaliation by nation-state actors could result). As a consequence, we expect such events to be fairly rare. The tail average outcome resulted in 0.76 injuries per year.
- **Safety – Fatalities (SF):** Safety-related events stem exclusively from loss of operational control and not from data loss events. Events involving loss of operational control have been few in number, causing the data set for such events to be extremely small. Attackers may have incentives not to execute attacks that they otherwise could perform (for example, retaliation by nation-state actors could result). As a consequence, we expect such events to be fairly rare. The tail average outcome resulted in 0.04 fatalities per year. Additionally, fatalities would be most likely to occur for gas control systems and very unlikely for electric control

systems. Thus the likelihood of fatalities for electric control systems would be even less than the likelihood of injuries.

- **Environmental (E):** Environmental incidents are extremely unlikely to result from data loss events. While they could result from events where there is a loss of operational control, those events have been few in number. Attackers may have incentives not to perform attacks that they otherwise could perform, as noted in the Safety attribute. As a result, PG&E expects such events to be rare. The tail average outcome resulted in an environmental impact of $62,000 per year.
- **Reliability (R):** Reliability events would result exclusively from a loss of operational control. Events involving loss of operational control have been few in number. While attackers may have incentives not to execute attacks that they otherwise could perform (for example, retaliation by nation-state actors), they may also have incentives to execute such attack as part of a larger agenda (also often involving nation-state actors). As a consequence, PG&E expects such events to be fairly rare, but not as rare as safety-related events. The tail average outcome resulted in a reliability impact of 11.5 customer minutes a year.
- **Compliance (C):** Most compliance issues are independent of cyber attacks or potential cyber attacks. Moreover, compliance is no guarantee against cyber attacks, nor does it prevent some vulnerabilities that could be exploited (for example, weaknesses in operating systems or applications). The tail average outcome resulted in a $333,000 per year in possible compliance impacts per year.
- **Trust (T):** The impacts of a cyber attack on PG&E's ability to maintain public confidence in its ability to deliver electric and gas services safety, reliably, and securely are likely to be extensive. This would be true both for a loss of operational control and for a loss of data. A data loss event would also erode customers' confidence in PG&E's ability to protect their personal information. Trust is defined by SME input with a minimum and maximum range for each sub-risk event. The tail average outcome from these inputs resulted in a 4.48 percent change per year in brand favorability.
- **Financial (F):** Costs to recover from a cyber attack are expected to be substantial, including attack containment, evaluation, remediation of previously unknown vulnerabilities, recovery, root cause analysis, and possible engagement of external resources to assist in response and recovery functions. This would be the case both for a loss of operational control and for a data loss event. The tail average outcome resulted in a $92 million per year financial impact.

III. 2016 Controls and Mitigations (2016 Recorded Costs)

Each of the controls and mitigations described in this section manages one or more drivers of the cyber-attack risk. Controls and mitigations are organized in programs aligned with the NIST CSF, which establishes the basic premises of an effective cybersecurity program and is recognized as industry best practice. PG&E has adopted this framework to enable a standardized, objective approach for developing our programs to reduce cyber-attack risk. The major programs (also referred to as domains) of the NIST CSF discussed in this chapter are: Identify, Protect, Detect, and Respond.

The majority of mitigation programs for 2016 focused on deployment of detective technologies, the inclusion of technologies to identify threats, and the creation of a round-the-clock security operations center to improve threat intelligence and response. The programs are constructed to contain both controls and mitigations.

C1 – Identify: Activities that develop the organizational understanding to manage cyber-attack risks to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions and the related cyber-attack risks enables the organization to focus and prioritize its mitigation efforts, thereby putting resources where the most risk reduction will be gained.

C2 – Protect: Activities that develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services, supporting the ability to limit or contain the impact of a cyber-attack event, reducing both the frequency and consequence of cyber attacks.

C3 – Detect: Activities that identify the occurrence of a potential cybersecurity event, enabling timely discovery of a cyber attack and reducing the potential consequence of the cyber attack.

C4 – Respond: Activities that enable effective evaluation of a potential cyber-attack event, and containment of the impact of a cyber attack again reducing the potential consequence of a cyber attack.

Table 18-1 below summarizes associated 2016 recorded costs associated with each control.

Table 18-1: Risk Controls and Mitigations 2016 Recorded Costs

#	Controls and Mitigations	Associated Driver and Consequence	Funding Source	2016 Recorded Expense ($000)	2016 Recorded Capital ($000)
C1	Identify	All Drivers	GRC TO GT&S	6,177 (E) 1,199 (E) 2 (E)	9,035 (C) 295 (C) 496 (C)
C2	Protect	All Drivers	GRC TO GT&S	2,383 (E) 47 (E) 1 (E)	9,249 (C) – (C) – (C)
C3	Detect	All Drivers	GRC TO GT&S	2,784 (E) 88 (E) – (E)	2,674 (C) – (C) – (C)
C4	Respond	All Drivers	GRC TO GT&S	935 (E) 20 (E) – (E)	2,908 (C) – (C) 711 (C)
TOTAL Expense and Capital				**13,636 (E)**	**25,368(C)**

IV. Current Mitigation Plan (2017-2019)

Mitigations for the years 2017-2019 are also aligned with the NIST CSF—Identify, Protect, Detect, and Respond programs. Because of previous investments in Identify, Detect, and Respond, a majority of expenditures in 2017 are focused on protective technologies and processes. This trend is maintained for the 2017-2019 time period and is consistent with PG&E's use of cyber-attack mitigation and control programs. Each mitigation within the NIST CSF programs addresses all key risk drivers: governance, business process, systems and infrastructure, and people and culture discussed above.

M1A – Identify: The Identify mitigation program is composed of six projects: Third-Party Risk Management; Critical Application Security Monitoring; Identity and Access Management (IAM) Product Enhancements; Next Generation Endpoint Security; Priority Applications Integration; and Vulnerability Management improvements.

- **Third-Party Risk Management:** The organization will implement an integrated vendor risk management system that enables PG&E to improve upon current labor-intensive third-party risk management processes and support new programs. The system will provide a central repository for all vendor risk assessments, including responses to questionnaires, assessment reports, assessment communications, and evidence. Customization provides all LOBs optimal visibility into their respective vendors' assessment status and risk profiles. This mitigation includes workflow configuration, data validation, integration processes, and training and awareness.
- **Critical Application Security Monitoring:** Build a prioritized list of application logs and develop a road map to onboard the priority logs into PG&E's log review and correlation platform for monitoring and analysis. The project will leverage potential

application logs as well as Information Technology asset management and other data. Logging from high-criticality applications will be prioritized for onboarding.

- **IAM Product Enhancements:** Expand the capabilities of the IAM solutions to support cloud identity management, developer security Operations, database integrations, cloud access security, DOE Part 810 export controls, unstructured high-risk data access management, and segregation of duties. The project also includes extending on-premise IAM solutions to cloud and enterprise mobility.
- **Next Generation Endpoint Security:** Create an end-point security strategy, architecture, configuration, and profiles to support the key operating systems in use at PG&E. The capability augments or replaces signature-based antivirus protection, which is no longer fully effective against malware and other types of attacks. The project evaluates technology controls and the role of policy and procedure controls in the endpoint strategy.
- **Priority Applications Integration:** Systems will be evaluated for risk of inappropriate logical access, particularly systems critical for Sarbanes-Oxley (SOX) compliance and systems critical for compliance with regulatory requirements for the custody of Customer Energy Usage Data.
- **Vulnerability Management:** Develop and implement a comprehensive solution for vulnerability and patch management process across all PG&E lines of business (LOB). The solution may include governance, tools, and/or workflows.

M2A – Protect: The Protect program is comprised of these projects: Application Integration; Auto Cloud Security; (Operational Data Network (ODN)) Security Improvements; Cloud Security Training; Customer Information Protection; Enterprise Password Vault; Gas Supervisory Control and Data Acquisition (SCADA) Network; and Catalog Privileged Accounts and Access to Critical Systems.

- **Application Integration:** Expands role-based LOB access controls and third-party account integration with access provisions for users in order to mitigate the risk of users with inappropriate access to high risk applications. Users will be granted access based only on the privileges required to do their job, and no more. Role-based access ensures that customers' personally identifiable information and corporate data are not lost due to incorrect user access.
- **Auto Cloud Security:** Designs and implements a collection of processes and tools for applications, computers, and storage and network deployment on the cloud in order to mitigate the risk of data stored in the cloud. The project also deploys capabilities to continuously test, detect, measure, and incrementally improve security to reduce risk.
- **ODN Security Improvements:** This is a multi-year project that will extend beyond 2019 into the 2020-2022 period. The first year will establish core security technologies and test their compatibility with OT devices. This will enable the development of technology architecture and designs to deploy in future years at Distribution Control Centers, transmission substations, distribution substations, and customer service centers. Technology deployed will address threats from a cyber

attack, allowing a response to an identified cyber attack to create separation zones to limit the impact of an attack and maintain substation automation to the rest of the territory.

- **Cloud Security Training:** Obtains security training courses for employees on cloud security in order to mitigate the risks of deploying and managing vendor-provided cloud systems. Additional training and job aids will be developed internally to expose development teams to security best practices in secure system development, operations, configuration management, vulnerability management, and data loss prevention.
- **Customer Information Protection:** Develops and implements a data security governance program to address and manage compliance and legal requirements to ensure that sensitive data is protected in alignment with the PG&E data classification framework, policies and standards. The organization will deploy technology to discover where sensitive information resides, and assess the health of the controls in place. Where controls are lacking, remediation measures will be identified and implemented in phases based on risk.
- **Enterprise Password Vault:** Provides complex passwords for the systems a user needs to access. This will reduce the risk of security incidents due to the use of common passwords.
- **Gas SCADA Network:** This is a mitigation completed in multiple phases, addressing asset management, network protection (segregation, reduce single point of failure), security monitoring, and technology evaluation and planning for operating system upgrades. Parts of this mitigation are dependent on the Security Analytics and Advanced Monitoring project.
- **Catalog Privileged Accounts and Access to Critical Systems:** Secures the enterprise network through identifying and cataloging individual users who have custody of critical PG&E logical and/or physical assets. The project will also identify users with privileged access or access to both physical and logical critical systems.

M3A – Detect: The Detect Program is comprised of the following projects: Mobile Threat Detection; Security Analytics and Advanced Monitoring Phase III; Security Analytics Enhancements; and Security Monitoring Capability Extension.

- **Mobile Threat Detection:** Implements comprehensive threat protection for Bring Your Own Device and Corporate-Owned Personally Enabled devices against mobile network, device, and application related cyber attacks. Also implemented will be a solution that monitors mobile devices in real time to detect known and unknown threats, analyzes any deviations from baseline behavior, and responds immediately.
- **Security Analytics and Advanced Monitoring Phase III:** Enhances cybersecurity monitoring technology, algorithms, tools, and processes to use improved techniques for discovery, logging, analysis, detection, and alerting. These enhancements will include different or improved statistical analysis, machine learning, or other forms of analytics and advanced monitoring.

- **Security Monitoring Capability Extension:** Accommodates organic growth in security monitoring of systems, of system attributes, and log retention. Accommodating this growth requires the addition of storage, network capacity, software licensing, and hardware.

M4A – Respond: The Respond Program is comprised of two projects: Advanced Persistent Threats (APT) Detection and Analysis Enhancement; and eDiscovery Capacity and Resilience Improvement.

- **APT Detection and Analysis Enhancement:** Improves event analysis and accelerates the detection of attacks coming from APT by extending the length of time that security event logs are retained. This will improve the ability to detect malicious activity from a range of possible sources allowing for a faster response and mitigating the overall impact of the attack.
- **eDiscovery Capability and Resilience Improvement:** Increases the capacity of the tool currently used for eDiscovery, and creates space for data backups from the tool. The system is used to investigate and respond to suspicious cyber activity. Increasing capacity will increase system resiliency when responding to a cyber attack.

Table 18-2 shows the associated costs for 2017-2019, based on the bundle of work under each domain.

Table 18-2: 2017-2019 Mitigation Work and Associated Costs

#	Mitigation Name	Start Date	End Date	Associated Driver	2017 Estimate ($000)	2018 Estimate ($000)	2019 Estimate ($000)
M1A	Identify	2017	2019	All Drivers	6,817 (C) 1,158 (E)	4,737 (C) 815 (E)	4,737 (C) 815 (E)
M2A	Protect	2017	2019	All Drivers	10,912 (C) 3,953 (E)	13,406 (C) 5,067 (E)	13,616 (C) 5,167 (E)
M3A	Detect	2017	2019	All Drivers	1,468 (C) 427 (E)	6,055 (C) 1,303 (E)	6,775 (C) 1,302 (E)
M4A	Respond	2017	2019	All Drivers	3,605 (C) 516 (E)	– (C) 42 (E)	– (C) 42 (E)
TOTAL Expense and Capital by Year					**22,802 (C) 6,054 (E)**	**24,198 (C) 7,227 (E)**	**25,128 (C) 7,326 (E)**

The mitigation programs listed above will address the four drivers, as discussed above, and more specifically they are expected to support the following objectives.

- The improved ability to isolate systems and networks affected by control failures, thus reducing their impact considerably (system infrastructure); and
- Better control over the use of confidential and sensitive data to ensure that only authorized individuals are able to access those categories of data (business process, people and culture and governance).

In 2017, improvements in network situational awareness and asset configuration management are being implemented with the goal of quicker root cause analysis and better estimation of recovery times in the event of a cyber attack on gas distribution or transmission control systems. In addition, improvements in identity and access management started in previous years will be completed to ensure that PG&E employees and contractors have only the access they need to do their jobs. The mitigation program to comprehensively protect customer information begins in 2017 and will continue into subsequent years.

In 2018 and 2019, improvements in network protection, including protection of field devices, are to be implemented. Additional improvements in asset configuration management are also scheduled. These changes are intended to enable better localization of any control failures that could occur from a cyber attack on gas distribution or transmission control systems, thus reducing their duration and impact. Even so, threats continue to evolve and protective and detective practices must evolve as well to effectively counter those threats. Given the dynamic nature of cybersecurity and, in particular, cyber threats, impacts and mitigations must be re-evaluated at least yearly. The customer information protection mitigation program will also continue in order to advance improvements in preventing unauthorized access to customer data. In addition, as cloud computing becomes more important at PG&E, mitigation initiatives are planned to reduce the risks to data stored in the cloud.

V. Proposed Mitigation Plan (2020-2022)

The proposed mitigations below are a continuation of the mitigations listed above in 2017-2019. Consistent with previous years, cyber-attack risk mitigations for 2020-2022 are organized into four programs that organize mitigation projects to extend and improve controls in groupings that are in alignment with the NIST CSF. Similar to the previous section, each of the programs address all of the drivers of Governance, Business Process, Systems and Infrastructure, and People and Culture. Additionally, it is important to recognize the fluidity of these programs, which will be reprioritized as the threat landscape changes. Detailed descriptions of each of the four programs follow below.

M1B – Identify: The Identify program is comprised of five projects: Citizen Developer Models; Third-Party Security and Risk Management; IAM Product Enhancements; Enhance Cyber Reporting; and Future Generation Endpoint Security Program.

- **Citizen Developer Models:** To secure the enterprise network the organization will identify and catalog individual users in all LOBs with significant critical PG&E logical and/or physical assets. The organization will ensure that common standards, repositories, version control, testing standards, testing tools, and integration with agile code pipelines are developed and implemented. These models will enable

each LOB to perform some of its own application development services. Citizen developer models will also support the use of consistently secure coding practices across multiple development organizations, thereby reducing the risk of insecure code.

- **Third-Party Security and Risk Management:** This project will implement an integrated vendor risk management system that will enable PG&E to improve upon current labor-intensive third-party risk management processes, as well as supporting new programs. The system will provide a central repository for all vendor risk assessments. Customization will provide all LOBs optimal visibility into their respective vendors' assessment status and risk profiles. This mitigation includes workflow configuration, data validation, integration process and training and awareness. The improved business processes and repository of records provided by the initiative will permit a better understanding of the cybersecurity risks that vendors may present to PG&E.
- **IAM Product Enhancements:** This initiative expands the capabilities of the IAM solutions to support cloud identity management, developer security operations, high risk database integrations, cloud access security, DOE Part 810 export controls, unstructured high risk data access management, and segregation of duties. It includes extending on-premise IAM solutions to cloud and enterprise mobility. The capabilities enabled by this project will improve the quality of access control and reduce the risk of inappropriate access across multiple environments, including public cloud environments.
- **Enhance Cyber Reporting:** This project will permit cybersecurity analysts to spend more time responding to high-impact incidents, and less time on mundane administrative tasks. The current process to respond to an event requires labor-intensive steps to investigate the event, identify the event as an incident, perform forensics on the system, and upload event data so the proper response can be executed. This mitigation will assist analysts in identifying and responding to security events in a more efficient and timely manner. Timely response to cyber-attack events reduces the risk of higher impact to PG&E systems and data.
- **Future Generation Endpoint Security Program:** Aims to leverage technology improvements in the ability to detect, alert, prevent or block unwanted or malicious activity on endpoint computing devices. Unwanted activity might include unwanted system changes, code execution or network traffic. Endpoint computing devices might include computers, portable devices, or operational devices. The technology might leverage machine learning, behavioral analytics, or other techniques that improve protection effectiveness and value. The program would evaluate the computing environment, threat landscape, mitigation landscape available at the time to determine the best approach.

M2B – Protect: Through the following nine initiatives, PG&E will develop and implement safeguards to ensure delivery of critical infrastructure services.

- **ODN Security Improvements:** This project will implement technology to allow isolation of control failures caused by a cyber attack to create separation zones to limit the impact and maintain substation automation to the rest of the territory.

These improvements will reduce the reliability risk from the Integrated Planning cyber-attack failure scenario to a tolerable level by implementing access controls at remote sites, as well as securing the electric distribution system.

- **Gas SCADA Network Protection:** This project will address observations made by Gas Operations cybersecurity risk assessments. It is a mitigation in multiple phases, addressing asset management, network protection, security monitoring, technology evaluation and planning for operating system upgrades both before and during the RAMP period. Benefits include:
    - Enhanced situational awareness
    - Improved detection and response capabilities
    - Better preparation for future operational technologies
- **Customer Information Protection:** This set of projects will develop and implement a data security governance program that addresses and manages compliance and legal requirements to ensure that sensitive data is protected in alignment with the PG&E data classification framework, policies and standards. Technology will be deployed to discover sensitive information, and assess the health of the controls in place to protect that information. Where controls are lacking, remediation will be implemented in phases based on risks being mitigated. This initiative will reduce the risk of unauthorized access to data, malicious insider behavior, or other data breaches.
- **Smart Grid Security:** This project will advance the development and standardization of cybersecurity policies, procedures, and practices for the smart grid architecture and Advanced Metering Infrastructure (AMI). The project will ensure efficiencies in deploying new devices on the AMI network. It will also provide a real-time view of the state of the network, including the presence of rogue devices and malicious traffic. Strengthening the governance around network segmentation and hardening the perimeter will also be needed as additional stakeholders leverage the AMI network. Centralized governance will provide for consistent interactions among all stakeholders that use the AMI network to ensure effective security oversight.
- **Application Integration for Access Management:** To mitigate the risk of users having inappropriate access to high-risk applications, the project will expand role-based access controls to restrict workforce and third-party access to only the functions and data required to complete tasks or other job functions. The components of this initiative—application integration, third-party account integration, and control of user access based on roles and responsibilities—will reduce the risk of inappropriate access to high-risk data.
- **Patch Automation:** This project will deploy technology that enables a single, integrated patch management and automation solution to improve automation of patching for high and medium risk non-critical systems. The application of patches across all PG&E systems is labor-intensive and time-consuming. This program will automate the patching of critical and high impact systems. This mitigation will reduce time and labor spent on applying patches which equates to cost savings as well.

- **Automate Cloud Security:** This initiative will mitigate cyber threats to high- and medium-risk data stored in the cloud. Actions to accomplish this objective will include designing and implementing processes and tools to ensure that applications and data in the cloud are secure. This project will also enable the ability to continuously test, detect, measure and incrementally improve controls to reduce risk. This effort will ensure that cloud services utilized by PG&E adhere to PG&E's security requirements. This initiative would obtain the necessary tools and services to ensure that cloud environments used by PG&E are secure.
- **Catalog Privileged Accounts and Access to Critical Systems:** To secure the enterprise network, this project will identify and catalog individual users with access to significant critical PG&E logical and/or physical assets. Users with privileged access or access to both physical and logical critical systems will also be identified. The project will also provide additional monitoring and validation of user access to prevent and detect potential incidents.
- **Network Access Control (NAC):** The goal of this project is to implement NAC across PG&E's corporate network. Implementation of a NAC solution will enable PG&E to identify and permit access from only trusted devices to PG&E's network. It would also enable the ability to direct untrusted devices to a guest network to mitigate the risk they pose to devices that possess a higher level of trust.

M3B – Detect: The projects that comprise the mitigations in Detect are: Identity Analytics; Enterprise User and Entity Behavior Analytics; Security Analytics and Advanced Monitoring Phase III; Security Analytics and Advanced Monitoring Enhancements; Security Monitoring Lifecycle; and Security Monitoring Capacity Extension.

- **Identity Analytics:** This project will implement tools to monitor user and administrator activity. By monitoring these activities, the system learns the level of access required to perform specific job functions. It will then suggest an access profile that reduces access that is not needed to perform job functions. This capability will reduce the chance of granting excessive access to an individual, and reduces the risk of insider threats. These tools will also improve the efficiency of onboarding employees, maintaining and removing access credentials, and the ability to manage credentials for systems that are critical for SOX compliance.
- **Enterprise User and Entity Behavior Analytics:** This project will correlate user activity with other entities such as managed and unmanaged endpoints, applications (including cloud, mobile and other on-premise applications), networks, and external threats. Such correlation will identify intentional and unintentional insider actions that violate data usage policies. Tools deployed for this purpose will also proactively identify and enable an effective response to incidents in which data is sent outside PG&E with malicious intent (for example, data theft) by establishing a baseline of expected behaviors within a job function and flagging deviations from that baseline for further review.
- **Security Analytics and Advanced Monitoring Phase III:** The PG&E Threat Intelligence organization will continue to build out the SIOC. In this phase, the SIOC

will integrate and consolidate cybersecurity and physical security day-to-day operations by insourcing security analytics. The organization will obtain additional software licenses and add capacity to perform analytics with existing tools. The mitigation includes plans to add new tools with monitoring, detection, and analytics capabilities. Furthermore, this initiative will develop human process workflows that incorporate the security analytics into day-to-day operations. PG&E previously engaged a vendor for security event analysis, but the services provided by the vendor did not enable a holistic view of both cyber and physical security. Insourcing is an opportunity to improve the quality of security event detection and analysis, thereby enabling PG&E to detect more events, gain deeper insight into the events, and respond to them more quickly and more effectively. Activities planned for this phase also will improve collaboration between cybersecurity and physical security personnel and systems to improve the effectiveness of both functions.

- **Security Analytics and Advanced Monitoring Enhancements:** This set of projects will enhance cybersecurity monitoring technology, algorithms, tools, and processes to use improved techniques for discovery, logging, analysis, detection, and alerting. These enhancements will include different and improved statistical analysis, machine learning, or other forms of analytics and advanced monitoring to improve the effectiveness and efficiency of security analytics and monitoring in detecting cyber attacks.
- **Security Monitoring Lifecycle:** To maintain PG&E's monitoring capabilities, this mitigation will replace or upgrade obsolete security monitoring hardware or software with supported and relevant technology as technology ages. This may include replacing one or more technology platforms. Obsolete systems increase security risk, as they can cease to function, operate poorly, or increase operating cost. Vendor license terms can also be modified over time, necessitating changes to maintain valid licenses.
- **Security Monitoring Capacity Extension:** This set of activities will maintain and support sufficient security monitoring capacity through the addition of storage, network capacity, software licensing, and hardware (virtual or physical). Existing and anticipated growth will mandate additional monitoring capacity to sustain existing business capabilities. Moreover, expanding the scope of systems logged and monitored and retaining logs over longer periods of time will improve monitoring and alerting capabilities and reduce blind spots.

M4B – Respond: The Respond mitigation includes three projects: Optimize Cyber Response and Incident Reports; Enhance Cybersecurity Labs and Forensics; and Cyber Response Automation.

- **Optimize Cyber Response:** This project will enable security analysts to analyze and identify security incidents more effectively. A large number of events coming from multiple sources may need to be examined and cross-referenced in order to identify a security incident. Tools to automate the identification of incidents from events across multiple systems will reduce the time required for security analysts to perform the tasks needed to determine the appropriate response actions. Thus, security analysts can focus on responding to events more quickly. Timely event

response can lessen the impact of an event. This project will deploy technology that will aggregate events from disparate systems to determine if a cybersecurity incident has occurred. Typical systems that report events include anti-virus, firewalls, and data loss prevention agents. Operational systems can also report potential security events.

- **Enhance Cybersecurity Labs and Forensics:** PG&E will procure and build an in-house test lab to evaluate and configure monitoring and cybersecurity forensics tools. The lab would include systems that are representative of common PG&E environments. The mitigations enable testing of current forensics, monitoring, detection and alerting tools. These tools need to be tested for compatibility, to avoid outages of information technology or OT systems, as well as enabling the tools to be optimized before they are deployed in a real-time environment.
- **Cyber Response Automation:** Response automation will apply technologies that can identify common cyber incidents, quarantine an affected system or computer, and begin remediation. Timely response to events can reduce the impact of a security incident to PG&E systems. Response automation will provide effective incident mitigation to return a system or computer back to normal operations without waiting for a security analyst to respond. This allows security analysts to investigate and determine the root causes of more complex events, and allows the system or computer to return to service sooner.

Table 18-3 summarizes the mitigations' associated drivers and associated estimated costs for each year. The Risk Spend Efficiency (RSE) metric is not applied to the cyber-attack risk because of the complex and innovative nature of the attack methods which make estimating risk reduction a challenge.

Table 18-3: Proposed Mitigation Plan and Associated Costs

#	Mitigation Name	TA RSE (Units/$M)	EV RSE (Units/$M)	Start Date	End Date	Associated Driver #	2020Estimate ($000)	2021 Estimate ($000)	2022 Estimate ($000)
M1B	Identify	N/A	N/A	2020	2022	All Drivers	1,953 (C) 525 (E)	3,000 (C) 2,135 (E)	2,600 (C) 1,150 (E)
M2B	Protect	N/A	N/A	2020	2022	All Drivers	15,624 (C) 4,093 (E)	14,000 (C) 4,540 (E)	13,585 (C) 6,036 (E)
M3B	Detect	N/A	N/A	2020	2022	All Drivers	5,673 (C) 1,335 (E)	4,200 (C) 1,869 (E)	4,940 (C) 2,470 (E)
M4B	Respond	N/A	N/A	2020	2022	All Drivers	2,976 (C) 642 (E)	3,000 (C) 777 (E)	2,210 (C) 1,050 (E)
TOTAL Expense and Capital by Year							**26,226 (C) 6,595 (E)**	**24,200 (C) 9,321 (E)**	**23,335 (C) 10,706 (E)**

VI. Alternatives Analysis

While assessing all of the mitigations for cyber-attack risk, PG&E developed two alternative plans to the proposed mitigation plan. Alternative Plan 1 increases the scope and cost of mitigation programs while Alternative Plan 2 decreases scope and cost. Both plans are shown in Tables 18-4 and 18-5.

Alternative Plans 1 and 2 incorporate all four of the mitigation programs, with specific projects within the programs changing either pace and scope for each alternative. To maintain consistency with the previous sections of this discussion, this section presents each alternative on a program-by-program basis, with the two alternatives being directly compared within each program.

Table 18-4: Mitigation List

#	Mitigation	Proposed Plan	Alternative Plan 1	Alternative Plan 2	WP #
M1B	Identify	X			WP 18-2
M2B	Protect	x			WP 18-6
M3B	Detect	x			WP 18-13
M4B	Respond	X			WP 18-18
M1C	Identify		X		WP 18-2
M2C	Protect		X		WP 18-6
M3C	Detect		X		WP 18-13
M4C	Respond		X		WP 18-18
M1D	Identify			X	WP 18-2
M2D	Protect			X	WP 18-6
M3D	Detect			X	WP 18-13
M4D	Respond			X	WP 18-18

Table 18-5 below illustrates the key changes in our alternatives. Each alternative is a more of or less of approach and the chart below details which of the projects would actually change in each program.

Table 18-5: Alternative Plans

Proposed Mitigation Program	Alternative One	Alternative Two
Identify *($11.4 million Proposed Over RAMP Period)*	Increase scope of IAM Product Enhancements from high-risk systems to high- and medium-risk systems. Would have reduced risk for medium-risk systems as well as high-risk system but with increased execution risk because of greater scope. Increases cost by approximately $1 million.	Reduce scope of Enhanced Cyber Reporting, giving employees fewer tools to identify cyber-attack events. Reduces cost by approximately $0.33 million.
Protect *($57.9 million Proposed Over RAMP Period)*	Increase scope of Patch Automation to cover non-critical systems as well as critical systems. Expand Automate Cloud Security to migrate low-risk data in addition to medium- and high-risk data. Total increased cost of approximately $9.5 million.	Eliminate NAC project, increasing risk of unauthorized devices connecting to PG&E networks. Reduces cost by approximately $6 million.
Detect *($20.5 million Proposed Over RAMP Period)*	Increase scope of Security Monitoring Lifecycle and Security Monitoring Capability Extension to deploy additional, potentially unproven technologies. Total increased cost of approximately $4.1 million.	Reduce scope of Security Analytics and Advanced Monitoring Enhancements, deploying fewer technologies. Reduces cost by approximately $5.6 million.
Respond *($10.7 million Proposed Over RAMP Period)*	Increase scope of Enhance Cybersecurity Labs and Forensics to permit more tools to be evaluated for compatibility with the PG&E environment and for effectiveness. Increases cost by approximately $1 million.	Reduce scope of Enhance Cybersecurity Labs and Forensics, reducing lab testing capacity and requiring triage to test only upgrades to critical tools. Decreased cost of approximately $.9 million.

A. Alternative Plan 1

Below are the mitigations considered for Alternative Plan 1.

M1C – Identify: This alternative would have increased the amount spent on IAM Product Enhancements by approximately $1 million during the RAMP period, while retaining proposed spending for all other projects in this mitigation program.

This additional spend would expand the scope of IAM Enhancements and further expand the capabilities of the proposed solution to include medium-risk database integrations and medium-risk data access management of unstructured data. This would have reduced risk across high and medium systems compared to targeting only high-risk systems. PG&E chose not to implement this scope in our proposed scenario in order to utilize lessons learned during deployment of enhancements to only high-risk systems, thus enabling more efficient deployment among lower-risk systems after the RAMP period (post-2022).

M2C - Protect: The first alternative scenario would have increased the scope of the Patch Automation project by approximately $7.6 million and the Automate Cloud Security project by approximately $1.9 million while retaining the same scope for the other projects in the proposed mitigation program. The changes that were considered for the two projects are described in more detail in the following paragraphs.

- **Patch Automation** – The increase in spending for this project would have allowed deployment of a single patch management and automation solution. In the current environment we have multiple patch management solutions that support different operating systems. Moving to a single patch management solution could have improved automation of patching for all non-critical systems, expanding the scope of this project. This alternative would have covered non-critical systems that can be used to launch attacks against more critical systems. PG&E does not recommend this alternative for the 2020-2022 RAMP period because the increased costs would not provide a significant reduction in risk for safety-critical systems.
- **Automate Cloud Security** – The increase in spending for this project would have expanded the scope of the project by mitigating low-risk data in addition to high- and medium-risk data stored in the cloud. We don't recommend this alternative because the resulting risk reduction would be minimal compared to the investment required.

M3C – Detect: This alternative would have increased the amount spent on Security Monitoring Lifecycle by approximately $2.15 million and Security Monitoring Capability Extension by approximately $2 million while retaining proposed spending for all other projects in this mitigation program.

Increasing spend for these programs would have allowed PG&E to deploy emerging yet unproven technologies and would most likely have led to replacing the existing technology platform for this purpose. Any such platform could offer additional tools and capabilities to reduce the impact of cyber risk. However, immature technologies also introduce the risk of incorrect categorization of cyber events as potential cyber attacks. Because of the probability of this additional risk, PG&E recommends this type of scope expansion in the future, when emerging technologies have had the opportunity to mature.

M4C – Respond: This alternative would have increased the amount spent for the project to Enhance Cybersecurity Labs and Forensics by approximately $1 million, while retaining proposed spending for all other projects in this mitigation program.

This alternative would have included more systems that could have been tested in the lab for compatibility and effectiveness with new monitoring tools. The

RAMP proposal focuses on systems that are critical to safety or are otherwise common in the PG&E environment. This alternative would have expanded the scope to systems that are not common but still perform key business functions. PG&E's evaluation was that this expansion of scope did not meaningfully reduce the security or reliability impacts of cyber-attack risk and could be explored at a later time.

Table 18-6: Alternative Plan 1 and Associated Costs

#	Mitigation Name	TA RSE (Units/$M)	EV RSE (Units/$M)	Start Date	End Date	Associated Driver	2020 Estimate ($000)	2021 Estimate ($000)	2022 Estimate ($000)
M1C	Identify	N/A	N/A	2020	2022	All Drivers	1,953 (C) 525 (E)	3,000 (C) 2,135 (E)	3,600 (C) 1,150 (E)
M2C	Protect	N/A	N/A	2020	2022	All Drivers	15,624 (C) 7,843 (E)	14,000 (C) 7,790 (E)	13,585 (C) 8,536 (E)
M3C	Detect	N/A	N/A	2020	2022	All Drivers	6,848 (C) 1,635 (E)	5,200 (C) 2,399 (E)	5,490 (C) 2,970 (E)
M4C	Respond	N/A	N/A	2020	2022	All Drivers	3,082 (C) 892 (E)	3,300 (C) 952 (E)	2,330 (C) 1,150 (E)
TOTAL Expense and Capital by Year							**27,507 (C) 10,895 (E)**	**25,500 (C) 13,276 (E)**	**25,005(C) 13,806 (E)**

B. Alternative Plan 2

Below are the programs proposed for Alternative Plan 2.

M1D – Identify: This alternative would have reduced spending on the Enhance Cyber Reporting project during the RAMP period by approximately $330,000, while retaining proposed spending for all other projects in this mitigation program.

Considering potential restraints on funding, PG&E examined what could be reduced in this program. The Enhance Cyber Reporting project was identified as the only project in this mitigation program that could have been reduced with minimal impact to cyber-attack risk. Reducing Enhanced Cyber Reporting would have given employees fewer tools to identify cyber events and cyber attacks efficiently and consistently. This would require the employees to make up for the lack of automation by spending more effort on routine and administrative tasks not reducing the impact of a cyber-attack risk event and possibly increasing the impact of such an event.

M2D – Protect: This alternative would have eliminated the NAC project by approximately $6 million while retaining proposed spending for all other projects in this mitigation program.

This alternative was considered because of the complexity of NAC deployment. Eliminating NAC would have allowed unauthorized devices greater opportunity to compromise PG&E systems by allowing direct access to our corporate network resulting in an increased risk of cyber attack. The NAC project is designed to reduce that risk by directing devices not meeting PG&E security requirements to a guest network with minimal access to PG&E systems. Eliminating a NAC deployment would eliminate this capability. Thus, PG&E does not recommend this alternative because it would have relinquished an opportunity to substantially reduce cyber-attack risk.

M3D – Detect: This alternative would have reduced proposed spending for Security Analytics and Advanced Monitoring Enhancements Phase III by approximately $5.6 million while retaining proposed spending for all other projects in this mitigation program.

The justification for this alternative would have been to reduce costs and provide more time for the Security Analytics and Advanced Monitoring Phase III project to mature in order to obtain efficiencies in later deployments. However, delaying this project would have also prevented PG&E from leveraging new capabilities that could have improved the likelihood of detecting advanced cyber attacks.

M4D – Respond: This alternative would have reduced proposed spending for the project to Enhance Cybersecurity Labs and Forensics by approximately $.9 million, while retaining proposed spending for all other projects in this mitigation program.

This alternative would have decreased the capacity of the lab compared to the RAMP proposal, thus allowing PG&E to test only upgrades to critical tools and not evaluate new tools and technologies except on a best-effort basis. This alternative would have resulted in delays in applying updates to tools not deemed critical, reducing forensic response capabilities and potentially increasing the impact of a cyber-attack risk event. Additionally, this alternative would have delayed evaluations of emerging tools and technologies resulting in slower adoption and delayed risk mitigations thereby also increasing the impact of a cyber-attack risk event.

Table 18-7: Alternative Plan 2 and Associated Costs

#	Mitigation Name	TA RSE (Units/$M)	EV RSE (Units/$M)	Start Date	End Date	Associated Driver	2020 Estimate ($000)	2021 Estimate ($000)	2022 Estimate ($000)
M1D	Identify	N/A	N/A	2020	2022	D1,D2,D3,D4	1,953 (C) 450 (E)	3,000 (C) 2,030 (E)	2,600 (C) 1,000 (E)
M2D	Protect	N/A	N/A	2020	2022	D1,D2,D3,D4	13,764 (C) 3,593 (E)	12,000 (C) 3,840 (E)	13,585 (C) 5,036 (E)
M3D	Detect	N/A	N/A	2020	2022	D1,D2,D3,D4	4,743 (C) 1,185 (E)	3,200 (C) 1,659 (E)	2,340 (C) 1,770 (E)
M4D	Respond	N/A	N/A	2020	2022	D1,D2,D3,D4	2,632 (C) 642 (E)	2,700 (C) 701 (E)	2,030 (C) 1,050 (E)
TOTAL Expense and Capital by Year							**23,092 (C) 5,870 (E)**	**20,900 (C) 8,230(E)**	**20,555 (C) 8,856 (E)**

VII. Metrics

Proposed accountability metrics include the following, related to the proposed mitigations and drivers mitigated:

The publicly available metrics that measure the cyber-attack risk are as follows:

- Vulnerability Ticket Management – shows the high severity vulnerability ticket average age which measures the average amount of time in days of all currently open high-severity tickets.
- Phishing Click Through Rate – rate at which the organization clicks on links in internally-generated test phishing emails.

The metrics in this section are currently in use. These metrics are being revised and will be reassessed at the end of 2017 for future use or replacement. They are indicators of the overall risk and not necessarily of each mitigation's effectiveness.

VIII. Next Steps

The next steps toward improving PG&E's understanding and analysis for cyber-attack risk include researching best practices on obtaining event data specific to OT systems, such as those that govern electric and gas control systems, and industry agreement on the mapping of metrics to specific controls. There are challenges to obtaining this data however. As an example, the category of cyber-attack threats known as APT, specifically relevant to utilities, incorporates stealth by its very nature, thus making it impossible to gather data on potential attacks of this type. All known APT attacks are suspected to have support from nation states, which find it advantageous to maintain their attack capabilities in reserve. There is more data relating to attacks that cause a loss of information but, even in those attacks, victims often do not disclose information publicly in an attempt to limit legal liabilities. Currently, metrics focus on the day-to-day

operations of protective systems or on compliance and, to this point, have not been correlated with the probability of events.

As discussed, cyber-attack risk is distinctive among risks to PG&E because that risk is actively exploited by adversaries applying ever-increasing levels of skill to attempt to breach PG&E systems and data. Legacy systems, particularly operational technology, are especially difficult to secure because standard approaches such as frequent patching and updates may sometimes conflict with imperatives to maintain the availability and reliability of the gas and electric systems. The cybersecurity program must balance these imperatives and, in appropriate situations, implement alternative controls to compensate for challenges in deploying standard controls. Operational technology systems may have a particularly large impact on the safety of the gas and electric systems. Ensuring the security of customer data is also important, requiring measures to be taken to protect against data loss. In addition, the program must protect innovative technologies such as cloud computing, SmartMeter™ devices, distributed generation, the Internet of Things, and future platforms not yet envisioned. Innovations in technology combined with innovation by our adversaries will require continual improvements in the PG&E cybersecurity program, requiring a risk-informed program that is recognized as a leader among utilities.