

San Diego Gas & Electric Company (U 902 M)  
Proceeding: 2024 General Rate Case  
Application: A.22-05-015 /-016 (consolidated)  
Exhibit: SDG&E-225-E

**REBUTTAL TESTIMONY OF  
BEN GORDON AND WILLIAM J. EXON  
INFORMATION TECHNOLOGY**

**ERRATA**

**BEFORE THE PUBLIC UTILITIES COMMISSION  
OF THE STATE OF CALIFORNIA**



**June 2023**

## TABLE OF CONTENTS

I.	SUMMARY OF DIFFERENCES .....	1
II.	INTRODUCTION .....	1
	A. Cal Advocates .....	2
	B. TURN.....	3
	C. UCAN .....	4
III.	GENERAL REBUTTAL .....	4
	A. TECHNOLOGY OBSOLESCENCE .....	4
IV.	REBUTTAL TO PARTIES’ O&M PROPOSALS.....	7
	A. Non-Shared Services O&M .....	7
	1. Customer Information System (CIS) Replacement ongoing expenditures .....	7
	a. Cal Advocates .....	7
	2. Customer Information System Balancing Account (CISBA).....	10
	a. Cal Advocates .....	10
	B. Shared Services O&M .....	11
	1. Smart Meter 2.0 Telecom Data Plan expenditures .....	11
	a. CAL ADVOCATES .....	11
	b. UCAN .....	13
V.	REBUTTAL TO PARTIES’ CAPITAL PROPOSALS .....	13
	A. General Rebuttal to Cal Advocates IT Capital Forecast Testimony.....	14
	B. Smart Meter 2.0 (WP# 218810).....	15
	1. CAL ADVOCATES .....	16
	2. TURN.....	17
	3. UCAN .....	18
	C. Smart Meter Product/Upgrade – (WP# 00900D & WP# 00900E).....	19
	1. Cal Advocates .....	22
	2. UCAN .....	23
	D. Field Service Delivery (FSD) (RAMP) – (WP# 00920AI & WP# 00920T).....	24
	1. CAL ADVOCATES .....	25
	2. TURN.....	26
	3. UCAN .....	27
	E. Field Mobility Development (WP# 00920AS).....	28
	1. UCAN .....	28
	F. CIS Regulatory & Enhancements – (WP# 00903E, WP# 00903F, WP# 00903G) .....	29
	1. Cal Advocates .....	34
	2. TURN.....	34

3.	UCAN .....	36
G.	Contact Center of the Future (CCotF) – (WP# 00903B) .....	36
1.	Cal Advocates .....	38
2.	TURN.....	39
3.	UCAN .....	40
H.	Digital Workspace (RAMP) – (WP# 00908B) .....	40
1.	UCAN .....	41
I.	Virtual Desktop Infrastructure (VDI) Expansion – Phase 2 (RAMP) – (WP# 00908C).....	42
1.	UCAN .....	43
J.	Select Projects UCAN Challenged for Technology Obsolescence.....	44
1.	UCAN .....	44
VI.	CONCLUSION.....	48

## APPENDICES

APPENDIX A – GLOSSARY OF TERMS

APPENDIX B – GLOSSARY OF DEFINITIONS

APPENDIX C – INDUSTRY EXPERT RESEARCH & REFERENCES

APPENDIX D – ILLUSTRATION OF IT PROJECT LIFECYCLE

**REBUTTAL TESTIMONY OF  
BEN GORDON AND WILLIAM J. EXON  
(INFORMATION TECHNOLOGY)**

**I. SUMMARY OF DIFFERENCES**

<b>TOTAL O&amp;M - Constant 2021 (\$000)</b>			
	<b>Base Year</b>	<b>Test Year</b>	<b>Change</b>
SDG&E	97,995	110,418	12,423
CAL ADVOCATES	97,995	97,226	(769)
TURN	97,995	110,418	12,423
UCAN	97,995	108,242	10,247

<b>TOTAL CAPITAL - Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	220,012	208,793	214,186	642,991	N/A
CAL ADVOCATES <sup>1</sup>	217,866	190,886	175,397	584,149	(58,842)
TURN <sup>2</sup>	183,087	131,115	102,874	417,076	(225,915)
UCAN <sup>3</sup>	Unclear	Unclear	Unclear	Unclear	

**II. INTRODUCTION**

In this rebuttal testimony, William J. Exon (1) adopts the direct testimony of Tia Ballard and Operations and Maintenance (O&M) work papers supporting San Diego Gas Electric's (SDG&E) request for Information Technology (IT) O&M costs.<sup>4</sup> This rebuttal also (2) addresses the following testimony from other parties:

- The Public Advocates Office of the California Public Utilities Commission (Cal Advocates), as submitted by Mariana Campbell (Exhibit CA-10), dated March 27, 2023.

<sup>1</sup> Ex. CA-10 (Testimony of Mariana Campbell on behalf of Cal Advocates), March 27, 2023, at 33, Table 10-23.

<sup>2</sup> TURN did not provide an overall Capital forecast recommendation. SDG&E derived the TURN forecast by subtracting TURN's recommendation to deny certain projects from the SDG&E Capital forecast. (See Ex. TURN-09 (Prepared Testimony of David Cheng submitted on behalf of TURN), March 27, 2023, at 25-27, 30, 33.)

<sup>3</sup> UCAN did not specify an overall Capital forecast expenditure recommendation. UCAN makes various recommendations in various years that are addressed in Section V, below, of this testimony.

<sup>4</sup> Ex. SDG&E-25, Chapter 2 (Prepared Direct Testimony of Tia L. Ballard (O&M Information Technology)), May 2022; Ex SDG&E-25-WP (Workpapers to Prepared Testimony of Tia L. Ballard), May 2022, adopted by William J. Exon.

- 1 • Cal Advocates, as submitted by Mark Waterworth (Exhibit CA-11), dated March
- 2 27, 2023.
- 3 • The Utility Reform Network (TURN), as submitted by David Cheng (Exhibit TURN-
- 4 09), dated March 27, 2023.
- 5 • Utility Consumer’s Action Network (UCAN), as submitted by Jason Zeller,
- 6 dated March 27, 2023 (hereinafter, Ex. UCAN (Zeller)).
- 7 • UCAN, as submitted by Dr. Eric Woychik, dated March 27, 2023 (hereinafter,
- 8 Ex. UCAN (Woychik)).

9 As a preliminary matter, the absence of a response to any particular issue in this rebuttal  
10 testimony does not imply or constitute agreement by SDG&E with the proposal or contention made by  
11 these or other parties. The forecasts contained in SDG&E’s direct testimony, performed at the project  
12 level, are based on sound estimates of its revenue requirements at the time of testimony preparation.

13 **A. Cal Advocates<sup>5</sup>**

14 The following is a summary of Cal Advocates’ positions:

- 15 ■ A forecast of \$16.097 million for TY 2024 Non-Shared Services O&M
- 16 expenditures, a reduction of \$11.016 million from SDG&E’s forecast of
- 17 \$27.113 million relating to SDG&E’s O&M forecast expenditures for the

---

<sup>5</sup> As an initial note, Cal Advocates asserts that it “experienced unnecessary delays in analyzing and evaluating SoCalGas’s and SDG&E’s IT capital projects because the support and detailed breakdown of all costs for the projects were included in separate exhibits from the project justifications.” (Ex. CA-14 (Testimony of Refat Amin), March 27, 2023, at 4, fn. 9.) Cal Advocates then asks the Commission to order the Applicants to include the support and justification details in one place for ease of Cal Advocates review in future GRCs. SDG&E disagrees that the relief Cal Advocates requests is necessary or warranted. Applicants’ testimony is structured and provided by the witness that has knowledge of and is sponsoring the proposal and can attest to its accuracy. Business witnesses cover the business need of a proposed project because they are the subject matter expert for their business areas requirements and objectives, while the IT witness can attest to the technical justification and the costs and attributes of the associated project that the IT organization handles to develop, build and implement. SDG&E has structured its testimony in this manner in its previous GRCs without objection. Nor is there any prejudice to parties in having projects supported by the witness areas that possess the relevant evidence. In this GRC, Cal Advocates had 10 months from the time the Application was filed to the date of its testimony to analyze and evaluate Applicants’ IT projects. More time was afforded in this proceeding than contemplated by even the Commission in its Rate Case Plan decision. (See D.20-01-002, Appendix B (Schedule for the Transition from the Current Three-Year GRC Cycle to the Four-Year GRC Cycle).) Cal Advocates’ request should be rejected.

1 Customer Information System (CIS) Replacement on-going operations  
2 and maintenance.<sup>6</sup>

- 3 • A forecast of \$81.129 million for TY 2024 Shared Services O&M expenditures,  
4 a reduction of \$2.176 million from SDG&E's forecast of \$83.305 million  
5 relating to SDG&E's O&M forecast expenditures for the Smart Meter 2.0  
6 Telecom Data Plan.<sup>7</sup>
  - 7 ▪ A forecast of \$217.866 million for 2022 Capital expenditures, a reduction  
8 of \$2.146 million from SDG&E's forecast of \$220.012 million.<sup>8</sup>
  - 9 ▪ A forecast of \$190.886 million for 2023 Capital expenditures, a reduction  
10 of \$17.907 million from SDG&E's forecast of \$208.793 million.<sup>9</sup>
  - 11 ▪ A forecast of \$175.397 million for 2024 Capital expenditures, a reduction  
12 of \$38.789 million from SDG&E's forecast of \$214.186 million.<sup>10</sup>

13 **B. TURN**

14 The following is a summary of TURN's positions:

- 15 • TURN does not take issue with SDG&E's TY 2024 Non-Shared Services O&M  
16 forecast of \$27.113 million.
- 17 • TURN does not take issue with SDG&E's TY 2024 Shared Services O&M  
18 forecast of \$83.305 million.
- 19 • A forecast of \$183.087 million for 2022 Capital expenditures, a reduction of  
20 \$36.925 million from SDG&E's forecast of \$220.012 million.<sup>11</sup>
- 21 • A forecast of \$131.115 million for 2023 Capital expenditures, a reduction of  
22 \$77.678 million from SDG&E's forecast of \$208.793 million.<sup>12</sup>

---

<sup>6</sup> Ex. CA-11 (Waterworth) at 5:25-30, 57 (Table 11-28), 59:20-21.

<sup>7</sup> *Id.* at 57 (Table 11-28), 60:2-8.

<sup>8</sup> Ex. CA-10 (Campbell) at 33, Table 10-23.

<sup>9</sup> *Id.*

<sup>10</sup> *Id.*

<sup>11</sup> *See* footnote 2, *supra* (TURN did not provide an overall Capital forecast recommendation. SDG&E derived the TURN forecast by subtracting TURN's recommendation to deny certain projects from the SDG&E Capital forecast. (*See* Ex. TURN-09 (Cheng) at 25-27, 30, 33.))

<sup>12</sup> *Id.*

- 1           •       A forecast of \$102.874 million for 2024 Capital expenditures, a reduction of  
2                 \$111.312 million from SDG&E’s forecast of \$214.186 million.<sup>13</sup>

3           **C.     UCAN**

4           The following is a summary of UCAN’s positions:

- 5           •       UCAN does not take issue with SDG&E’s TY 2024 Non-Shared Services O&M  
6                 forecast of \$27.113 million.
- 7           •       A forecast of \$81.129 million for TY 2024 Shared Services O&M expenditures,  
8                 a reduction of \$2.176 million from SDG&E’s forecast of \$83.305 million  
9                 relating to SDG&E’s O&M forecast expenditures for the Smart Meter 2.0  
10                Telecom Data Plan.<sup>14</sup>
- 11          •       UCAN generally opposes SDG&E’s IT Capital forecast based on technology  
12                 obsolescence and stranded asset contentions but did not specify an overall  
13                 Capital forecast expenditure recommendation. UCAN makes various  
14                 recommendations on certain projects that are addressed in Section V of this  
15                 testimony.

16          **III.    GENERAL REBUTTAL**

17           **A.     TECHNOLOGY OBSOLESCENCE**

18           Eventual obsolescence, which impacts numerous industries, sparks creativity, innovation and  
19           change in society. That is not in itself bad or problematic. Technology is an industry of great change  
20           and innovation. SDG&E prudently manages these changes and accompanying obsolescence through  
21           the vetting and rigor of its technology selection, design, testing processes on the front end to meet its  
22           business and customer needs,<sup>15</sup> and by its actions upon implementation to regularly update and  
23           maintain that technology to maximize its lifespan. SDG&E invests in modern technologies as  
24           technology evolves, such as Cloud, machine learning, and artificial intelligence to streamline  
25           operations, increase performance, and provide our customers with innovative, digital solutions and

---

<sup>13</sup> *Id.*

<sup>14</sup> Ex. UCAN (Woychik) at 294:15-16. *See infra* at BG-WJE-13:5-16 identifying IT portion of O&M costs.

<sup>15</sup> *See* Appendix D, at BG-WE-D-1 (Illustration of IT Project Lifecycle as part of SDG&E Response to DR PAO-SDGE-043-LMW, Question 1.e.).

1 insights. SDG&E strategically and thoughtfully selects IT investments with the intention of improving  
2 safety, reliability, and efficiency for our customers not limited to a specific time-period.

3 Throughout its testimony, UCAN contends in various ways that SDG&E’s technology projects  
4 “will be obsolete, require replacement, and thus not be used and useful during the GRC period.”<sup>16</sup>  
5 UCAN’s unfounded assertions reveal UCAN’s misapprehension of the technology industry and the  
6 need for SDG&E to invest in technologies to mitigate technology obsolescence and to prepare for  
7 future regulatory and customer needs. As SDG&E demonstrated in its IT Policy testimony, the Test  
8 Year (TY) 2024 forecast focuses on a digital operating model, which will enable faster, more resilient,  
9 and innovative technology solutions for SDG&E and its customers.<sup>17</sup> SDG&E “Proactively Manage[s]  
10 Risk,” by “continuing to manage the technology lifecycle, by replacing unsupported technologies,  
11 ensuring the resiliency and recovery of technology systems and patching identified vulnerabilities,”<sup>18</sup> as  
12 one of the key pillars that underlies SDG&E’s IT capital forecast, and is deploying innovative  
13 technologies, such as Cloud-based solutions, which enable innovation and rapid development of  
14 solutions to meet Company and customer needs while “also provid[ing] high levels of availability,  
15 resiliency, and reduced risks due to hardware and software versions remaining current.”<sup>19</sup> Rather than  
16 the need for “assurances that these projects will avoid technological obsolescence,”<sup>20</sup> that UCAN  
17 expects, SDG&E is proactively managing the inevitability that all technology becomes obsolete at  
18 varying times and degrees.

19 As systems age, their reliability and efficiency decrease, and the risk of system failure increases.  
20 Technology industry expert Gartner notes, “All technology becomes obsolete and unsupported over  
21 time. Unsupported systems do not receive bug fixes, enhancements, and, most importantly, security  
22 patches — significantly increasing the risk of system compromise.”<sup>21</sup> Ensuring that systems are

---

<sup>16</sup> See, e.g., Ex. UCAN (Woychik) at 207:14-17, 279:22-280:1. UCAN provides no support for its statement that certain technology projects will be “obsolete or at best interim (useful for two years or less).” (*Id.* at 280:9-14.) SDG&E addresses UCAN’s assertions in Section V of this testimony.

<sup>17</sup> See Ex. SDG&E-25 Chapter 1 (Prepared Direct Testimony of Ben W. Gordon (Information Technology Policy)), May 2022, at BWG-2.

<sup>18</sup> *Id.*

<sup>19</sup> See *Id.* at BWG-4-5.

<sup>20</sup> Ex. UCAN (Woychik) at 304:9-10.

<sup>21</sup> Appendix C-1, Gartner, *Securing End-of-Support Production Systems*, March 15, 2023, at 1-2.



1 regularly updated and maintained to maximize their lifespan, as well as investing in technologies that  
2 are designed to meet the business and customer demands is prudent business practice.

3         Additionally, failure to address technology obsolescence increases the risk of unauthorized  
4 access to SDG&E’s confidential assets and customer data due to cybersecurity vulnerabilities in  
5 outdated technology. As noted by the United States Department of Homeland Security’s Cybersecurity  
6 and Infrastructure Security Agency (CISA), “Use of unsupported (or end-of-life) software in service of  
7 Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to  
8 national security, national economic security, and national public health and safety. This dangerous  
9 practice is especially egregious in technologies accessible from the Internet.”<sup>22</sup> UCAN’s misguided  
10 position on technology obsolescence, that the Commission should disallow SDG&E’s technology  
11 investments, could lead not only to increased risks, cybersecurity threats, and inefficiencies in our  
12 systems but could also have a direct impact in the delivery of reliable, safe, efficient, and secure  
13 services to customers.

14         UCAN also repeatedly contends that SDG&E is investing in technology for the short-term, to  
15 improve its bottom line, rather than making longer-term innovative technology investments that  
16 anticipate future needs.<sup>23</sup> UCAN’s statements lack support and are incorrect. UCAN fails to  
17 understand that SDG&E invests in technology that is requested and aligned with business needs and  
18 long-term technology roadmaps. The IT Division develops a proposed set of capital projects for the  
19 upcoming year by working with business clients to identify new technology capabilities to meet  
20 business and customer needs as well as working with the IT teams to identify technology lifecycle  
21 needs.<sup>24</sup> In addition to investing in regular updates to decrease vulnerability to its systems and  
22 maximizing their lifespan, SDG&E emphasizes the importance of investing in the right technologies  
23 with a clear understanding of business objectives and the ability to adapt to evolving customer and  
24 regulatory needs. A recent Gartner survey of utility company executives found utilities continued  
25 investment in digital technologies, recognizing “[t]he purpose of the investments is to ensure the ability  
26 to provide available, affordable, and acceptable services to the customers they serve. A sustainable  
27 utility future requires improved business resilience and the ability to quickly change to address new

---

<sup>22</sup> Appendix C-2, Department of Homeland Security, CISA, *Bad Practices*, at 2; also available at: <https://www.cisa.gov/stopransomware/bad-practices>.

<sup>23</sup> See, e.g., Ex. UCAN (Woychik) at 301.

<sup>24</sup> Ex. SDG&E-25, Chapter 2 (Information Technology) at TLB/WJE-22.

1 requirements arising from the energy transition and from increasing regulatory and political demands.  
 2 Utilities must shape-shift to increase resilience while maintaining productivity and efficiency.”<sup>25</sup>  
 3 Technology is a key enabler of safety, reliability, and compliance in the utility industry, and as  
 4 discussed in SDG&E’s IT Policy Testimony, “IT has developed a strategy to support the Company’s  
 5 mission of decarbonization and digitalization. Digitalization is central to SDG&E’s decarbonization  
 6 and Net Zero goals by improving operational service, efficiency, and safety, by providing real-time  
 7 information and cutting-edge analytics, benefiting operations, and customers.”<sup>26</sup>

8 **IV. REBUTTAL TO PARTIES’ O&M PROPOSALS**

9 **A. Non-Shared Services O&M**

10 **NON-SHARED O&M - Constant 2021 (\$000)**

	<b>Base Year</b>	<b>Test Year</b>	<b>Change</b>
SDG&E	19,808	27,113	7,305
CAL ADVOCATES	19,808	16,097 <sup>27</sup>	(3,711)
TURN	19,808	27,113 <sup>28</sup>	7,305
UCAN	19,808	27,113 <sup>29</sup>	7,305

11  
 12 Cal Advocates recommends adjusting out Non-Shared Services O&M forecast expenditures for  
 13 the Customer Information System (CIS) Replacement and requiring instead that the Customer  
 14 Information System Balancing Account (CISBA) remain open to track the ongoing CIS Replacement  
 15 costs.<sup>30</sup> SDG&E disagrees with Cal Advocates recommendations as discussed below.

16 **1. Customer Information System (CIS) Replacement ongoing expenditures**

17 **a. Cal Advocates**

18 Cal Advocates recommends an adjustment of \$11.016 million to SDG&E’s 2024 forecast  
 19 request for CIS Replacement ongoing expenditures. Cal Advocates bases its recommendation on its

<sup>25</sup> Appendix C-3, Gartner, *Research Roundup: Top 10 Trends Shaping the Utility Section in 2023*, January 25, 2023, at 2. See also Deloitte Insights, *Putting digital at the heart of strategy*, April 22, 2021, available at: <https://www2.deloitte.com/us/en/insights/topics/digital-transformation/digital-acceleration-in-a-changing-world.html>.

<sup>26</sup> Ex. SDG&E-25, Chapter 1 (Information Technology Policy) at BWG-1.

<sup>27</sup> Ex. CA-11 (Waterworth) at 57, Table 11-28.

<sup>28</sup> TURN did not take issue with SDG&E’s TY 2024 Non-Shared O&M forecast.

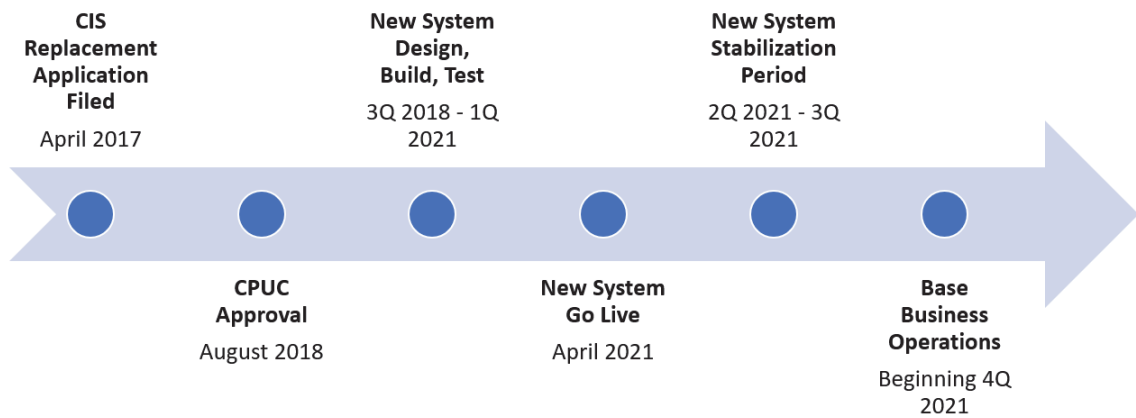
<sup>29</sup> UCAN did not take issue with SDG&E’s TY 2024 Non-Shared O&M forecast.

<sup>30</sup> Ex. CA-11 (Waterworth) at 59.

1 assertion that “SDG&E did not provide any actuals for 2022 and continues to base its estimate on a  
2 partial year of 2021 costs.”<sup>31</sup>

3 Cal Advocates is incorrect in its assessment. Regarding 2021 partial costs, Cal Advocates fails  
4 to recognize that the CIS Replacement Base Year costs represent a partial year, because the costs for  
5 this activity began in the last quarter of 2021. As depicted in Figure BG-WE – 1 prior to the last  
6 quarter of 2021, the CIS Replacement project was in the implementation phase and its costs were  
7 captured in the CISBA until the new CIS became operational.<sup>32</sup> Thus, the Base Year (2021) included  
8 only three months of actual cost for ongoing O&M once the CIS Replacement was implemented. The  
9 forecasted increase for the Test Year (2024) represents the incremental amount needed to normalize the  
10 Base Year to reflect a full calendar year (twelve months).

11 **Figure BG-WE – 1 [CIS Replacement Timeline]**



12 The table below illustrates how SDG&E normalized the 2021 Base Year costs by adjusting  
13 three months of on-going CIS Base Year costs to reflect a full calendar year and arrive at its Test Year  
14 forecast. The numbers in the table below demonstrate in simple terms how a full year of costs were  
15 calculated. Specifically, SDG&E took the Base Year Actuals, divided them by 3 to get a monthly  
16 average and then multiplied that number by 12 to arrive at a normalized value (i.e., 12 months). The  
17 approximate \$2 million difference to the full year forecast shown is primarily related to a contract  
18 renewal that would not incur costs until 2022, and therefore was not reflected in the Base Year.  
19 SDG&E attempted to clarify this misunderstanding with Cal Advocates in two separate data requests  
20 and two telephone conferences (September 22, 2022, and September 29, 2022) that was reflected and  
21

<sup>31</sup> *Id.* at 59:14-17.

<sup>32</sup> Ex. SDG&E-243 (Rebuttal Testimony of Jason Kupfersmid (Regulatory Accounts)).

noted in SDG&E’s response to PAO-SDGE-044-LMW and PAO-SDGE-075-LMW. SDG&E walked the Cal Advocates analyst through an explanation similar to that modeled in the table below explaining the simple logic behind the normalization (*i.e.*, annualizing) the 2021 historical costs so that the Base Year reflected a full year.

**Table BG -WE – 1 [Simple Cost Calculation]**

<b>CIS Base Year and Test Year Forecasted Costs Methodology - Constant 2021 (\$000)</b>					
	<b>2021 Base Year (3 months) Actual Costs</b>	<b>Implied Cost/Month</b>	<b>Implied 2021 Annual Cost</b>	<b>2024 TY Forecast</b>	<b>2024 Variance</b>
	<b>(A)</b>	<b>(B) = A / 3</b>	<b>(C) = B *12</b>	<b>(D)</b>	<b>(E) = D - C</b>
Labor	715	238	2,856	3,589	733
Non-Labor	2,230	743	8,916	10,372	1,456
<b>TOTAL</b>	<b>2,945</b>	<b>981</b>	<b>11,772</b>	<b>13,961</b>	<b>2,189</b>
<i>Variance to Base Year (D) - (A)</i>	<i>Variance to Base Year (D) - (A)</i>				

SDG&E provided its 2022 recorded expenditures on March 13, 2023, in compliance with *Administrative Law Judge’s Ruling Modifying The Procedural Schedule And Partly Denying Sempra Utilities’ Joint Motion To Amend The Assigned Commissioner’s Scoping Memorandum And Ruling*, dated December 6, 2022. A full year of CIS Replacement costs were part of those recorded expenditures. Although Cal Advocates complains that the provision of 2022 recorded expenditures under the Administrative Law Judge’s Ruling “leaves little time for Cal Advocates to review the response and edit its report (due March 27, 2023),”<sup>33</sup> this should not change the result. The GRC forecast was developed according to the Rate Case Plan, which does not contemplate the use of 2022 recorded data and the TY 2024 forecasts were not developed using 2022 recorded data. SDG&E is not permitted to revise its forecasts using that data, either up or down, once the application is filed. The 2022 recorded actual costs provide only another data point for intervenors to consider. Cal Advocates has provided no support for its recommendation, and it should therefore be disregarded. Any other result would severely underfund continued operations of the CIS Replacement,<sup>34</sup> which began operations near the end of the 2021 Base Year, see Figure BG-WE – 1 above.

<sup>33</sup> Ex. CA-11 (Waterworth) at 59:23-24.

<sup>34</sup> See Ex. SDG&E-16 (Prepared Direct Testimony of Therese C. Sacco (CIS Replacement Policy)) for a description of the CIS Replacement.

1                   **2.       Customer Information System Balancing Account (CISBA)**

2                   **a.       Cal Advocates**

3                   Cal Advocates also recommends that the CISBA remain open to track the CIS Replacement  
4 ongoing costs.<sup>35</sup> Cal Advocates apparently does not understand that the CISBA is no longer available  
5 for ongoing CIS Replacement costs. Ongoing O&M and capital costs for the new CIS are not recorded  
6 to the CISBA. As explained in Exhibit SDG&E-243 (Regulatory Accounts), only project  
7 implementation costs are authorized to be recorded to the CISBA, and since the implementation  
8 activities were complete in 2021, the account is closed to new charges.<sup>36</sup> SDG&E is not currently  
9 recording ongoing costs for the new CIS to the CISBA, as Cal Advocates appears to assume.<sup>37</sup>  
10 Ongoing O&M and capital costs for the new CIS are included in the 2021 Base Year (partial year) and  
11 incorporated into the TY 2024 forecast. Cal Advocates’ assertion that “[c]ontinuing to record these  
12 costs to the balancing account will allow for more accurate historic expenditures not present in  
13 SDG&E’s current estimate,”<sup>38</sup> is unfounded, contrary to the applicable Commission Decision,<sup>39</sup> and the  
14 opinion of the witness who is representing Cal Advocates on SDG&E Customer Services issues (Ex.  
15 CA-10 (Campbell). Although she cites to Mr. Waterworth’s chapter, Ms. Campbell states: “For  
16 SDG&E’s Customer Information System Balancing Account (CISBA), Cal Advocates does not oppose  
17 SDG&E’s proposed closure of the regulatory account.”<sup>40</sup>

18                   SDG&E has provided justification and support for the CIS Replacement ongoing costs in direct  
19 testimony (Ex. SDG&E-25, Section IV, Sub-Section B) and workpaper 1IT002.000 (Ex. SDG&E-25-  
20 WP). The CIS Replacement ongoing costs include labor, contractor resources, and software annual  
21 renewals to provide maintenance and support of the new CIS. Cal Advocates disallowance of \$11.016  
22 million to SDG&E’s TY 2024 Non-Shared Services forecast should be rejected and the Commission  
23 should adopt SDG&E’s forecast as reasonable.

---

<sup>35</sup> Ex. CA-11 (Waterworth), at 59:15-19.

<sup>36</sup> Ex. SDG&E-243 (Regulatory Accounts), Section III, Sub-Section A-1.

<sup>37</sup> Ex. CA-11 (Waterworth) at 59:17-19.

<sup>38</sup> *Id.*

<sup>39</sup> D.18-08-008; A.17-04-027, Settlement Agreement of SDG&E, ORA, UCAN, and TURN regarding Issues of SDG&E’s Customer Information System Replacement Program, January 24, 2018, Section III, Sub-Section C.

<sup>40</sup> Ex. CA-10 (Campbell) at 2:21-23.

1           **B. Shared Services O&M**

<b>SHARED O&amp;M – Constant 2021 (\$000)</b>			
	<b>Base Year</b>	<b>Test Year</b>	<b>Change</b>
SDG&E	78,187	83,305	5,118
CAL ADVOCATES	78,187	81,129	2,942
TURN	78,187	83,305	5,118
UCAN	78,187	81,129	2,942

- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- Cal Advocates recommends disallowing SDG&E’s 2024 Shared Services O&M forecast expenditures of \$2.176 million for the Smart Meter 2.0 Telecom Data Plan expenditures. Cal Advocates does not oppose the remainder of SDG&E’s TY 2024 Shared Services O&M forecast of \$81.129 million.
  - TURN does not challenge SDG&E’s TY 2024 Shared Services O&M forecast expenditure recommendation for \$83.305 million.
  - UCAN did not provide a TY 2024 O&M Shared Services forecast expenditure recommendation except for the Smart Meter 2.0 Telecom Data Plan forecast expenditures of \$2.176 million, which is part of the \$4.42 million O&M forecast reduction recommendation by UCAN.<sup>41</sup> UCAN does not take issue with the remainder of SDG&E’s TY 2024 Shared Services O&M forecast of \$81.129 million.

10           **1. Smart Meter 2.0 Telecom Data Plan expenditures**

11                   **a. CAL ADVOCATES**

12           Cal Advocates takes issue with the Test Year O&M forecast for the Smart Meter 2.0 Telecom  
13 Data Plan (SM 2.0) expenditures relating to the Smart Meter 2.0 Capital program. Cal Advocates  
14 recommends an adjustment of \$2.176 million to SDG&E’s 2024 forecast request. As noted in their  
15 testimony “Cal Advocates (per Ex. CA-10) recommends adjustment of the Smart Meter 2.0 project.  
16 Accordingly, Cal Advocates removes these normalized forecasted costs.”<sup>42</sup>

17           SDG&E disagrees with Cal Advocates’ adjustment. Neither of the Cal Advocates witnesses  
18 (CA-10 (Campbell) and CA-11 (Waterworth)) provide a substantive reason for their recommendation.  
19

20

---

21 <sup>41</sup> Ex. UCAN (Woychik) at 294:1-6.

22 <sup>42</sup> Ex. CA-11 (Waterworth) at 60:7-8.

1 Absent evidence, or even a rationale, the recommendation must be rejected. And, an adjustment on the  
2 premise of normalization alone is unwarranted.

3 SDG&E’s cost estimates were derivatives of actual pricing data received from the RFP process  
4 as described in the testimony of Customer Services – Field Operations (CSFO) (Ex. SDG&E-17-R).  
5 The pricing data, the projected quantities, and types of devices to be deployed in the SDG&E service  
6 territory were leveraged to develop the proposed telecom data plan expense. The telecom data plan  
7 costs are comprised of vendor fees, network backhaul and telecommunication tools and services.

8 These costs are necessary to achieve the purpose of the SM 2.0 project. First, without a telecom  
9 data plan, the new gas modules and electric meters will not be able to communicate with the head-end  
10 system – this is a fundamental facet to smart metering. This is equivalent to having a smartphone, but  
11 not being able to realize its full potential and capabilities due to lack of communication / telecom data  
12 plan. This defeats the purpose of smart metering, and the benefits associated with such systems.

13 Second, as part of SM 2.0, SDG&E expects to prepay the annual telecom data plan fees in each  
14 of the 10 years related to the new gas modules and electric meters. Prepayment of the telecom data plan  
15 offers cost protection to the rate payers from inflation. These costs will initially be recorded as prepaid  
16 O&M and amortized to O&M expense over the term of the agreement. The telecom data plan fees will  
17 grow as the number of new gas modules and electric meters grows. Therefore, the 2024 amount reflects  
18 an average of the 2024-2027 estimated O&M costs to normalize for the expected cost increase in the  
19 post-test years. Said another way, SDG&E has already normalized the cost. The calculation of the 2024  
20 amount is contained in the supplemental workpaper (2100- 0207.00, page 58) of Information  
21 Technology (Ex. SDG&E-25-WP).

22 As referenced in the rebuttal testimony of Customer Services Field Operations (CSFO) (Ex.  
23 SDG&E-217), the need for SM 2.0 is evident (including telecom data plans). And “Cal Advocates  
24 does not take issue with SDG&E’s justification for the current meter replacement initiative [SM2.0]”<sup>43</sup>

25 Based on the rebuttal testimony of CSFO and Cal Advocates acknowledgement of the need for  
26 SM 2.0, associated telecom data plan expenses will be required for the modules to communicate. Yet,  
27 Cal Advocates contradicts itself when it proposes to remove normalized forecasted O&M costs for the  
28 Smart Meter 2.0 Telecom Data Plan. The adjustment to the non-shared O&M forecast does not make  
29 sense and should be disregarded.

---

<sup>43</sup> Ex. CA-10 (Campbell) at 34:21-22.

1 For the reasons stated above, SDG&E requests Cal Advocates' disallowance of \$2.176 million  
2 to SDG&E's TY 2024 forecast be rejected. The Commission should find SDG&E's Shared Services  
3 O&M forecast costs to be reasonable and adopt SDG&E's forecast.

4 **b. UCAN**

5 UCAN also takes issue with SDG&E's Test Year O&M forecast for the Smart Meter 2.0  
6 Telecom Data Plan expenditures and recommends removal of \$2.176 million from SDG&E's 2024  
7 forecast request relating to the Smart Meter 2.0 Capital program. As noted in its testimony, UCAN  
8 asserts "O&M costs for 2024 of \$4.42 million and capital costs of \$58.46 million should be  
9 disallowed."<sup>44</sup> The \$2.176 million forecast for IT is included in the \$4.42 million O&M forecast  
10 reduction recommendation by UCAN. While UCAN does not appear to provide a justification for its  
11 recommendation specific to the telecom plan, as expressed above, without a telecom data plan, the new  
12 gas modules and electric meters will not be able to communicate with the head-end system. The SM 2.0  
13 Capital program is addressed in Section V (Sub-Section B) of this testimony and in the testimony of  
14 CSFO (Ex. SDG&E-17-R), which provides the business justification for the SM 2.0 Program. The  
15 rationale for adoption of the O&M costs for the telecom data plan is discussed immediately above in  
16 Section IV.B.1, and is likewise applicable here.

17 For the reasons stated above, UCAN's recommended disallowance of \$4.42 million to  
18 SDG&E's TY 2024 forecast lacks support and should be rejected. The Commission should adopt  
19 SDG&E's forecast as reasonable.

20 **V. REBUTTAL TO PARTIES' CAPITAL PROPOSALS**

<b>TOTAL CAPITAL - Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	220,012	208,793	214,186	642,991	N/A
CAL ADVOCATES	217,866	190,886	175,397	584,149	(58,842)
TURN	183,087	131,115	102,874	417,076	(225,915)
UCAN <sup>45</sup>	Unclear	Unclear	Unclear	Unclear	

21  
<sup>44</sup> Ex. UCAN (Woychik) at 13:3, 315-316.

<sup>45</sup> UCAN did not specify an overall Capital forecast expenditure recommendation. UCAN makes a variety of recommendations on certain projects that are addressed in Section V of this testimony.



1           **A.       General Rebuttal to Cal Advocates IT Capital Forecast Testimony**

- 2           •       Cal Advocates recommends two inconsistent forecasts for this TY 2024 GRC  
3           cycle in two different chapters of testimony (CA-10 (Campbell) and CA-11  
4           (Waterworth)). SDG&E adopted the forecast recommendation from CA-10.  
5           •       Cal Advocates also offers a third alternate recommendation for 2022, namely,  
6           Cal Advocates recommends adoption of SDG&E’s 2022 recorded adjusted  
7           Capital expenditures as the 2022 forecast.<sup>46</sup> Cal Advocates has not identified nor  
8           provided any analysis to support the recommendation.

9           With the exception of particular SDG&E Customer Services-related capital expenditure  
10          proposals, Cal Advocates does not dispute SDG&E's IT Capital Expenditure Forecasts.<sup>47</sup> In  
11          recommending reductions for certain Customer Service IT projects; however, Cal Advocates makes  
12          three contradictory recommendations. The inconsistencies appear in the Cal Advocates’ Chapter 10  
13          testimony for Customer Service Field Capital Expenditures and the Chapter 11 testimony for IT Capital  
14          Expenditures. While SDG&E will address the inconsistencies as it relates to each of the IT Capital  
15          projects forecasted respectively below, I address what appears to be a third and overarching  
16          recommendation here.

17          Although Cal Advocates complains it did not have sufficient time in the two weeks between  
18          SDG&E's service of 2022 recorded adjusted data and the date it served its testimony to incorporate that  
19          data into its forecast and R/O Model, Cal Advocates notes that the 2022 adjusted data is lower than  
20          SDG&E's 2022 forecast. Cal Advocates then “recommends this recorded figure be adopted for 2022.”<sup>48</sup>  
21          The request to substitute SDG&E's forecast for 2022 with the 2022 recorded adjusted 2022 data should  
22          be rejected. Cal Advocates admits it has done no analysis and provides no justification other than it  
23          saw a lower number and thought it should be applied. For the reasons stated previously,<sup>49</sup> and while  
24          recorded data may indicate lower spending than forecasted in some areas, it may also indicate higher  
25          spending than forecasted in others. The Rate Case Plan does not permit SDG&E to revise its forecasts  
26          using that data, either up or down, once the application is filed and SDG&E's forecasts were not

---

<sup>46</sup> Ex. CA-11 (Waterworth) at 66, n.108.

<sup>47</sup> Ex. CA-11 (Waterworth) at 67, Table 11-34.

<sup>48</sup> Ex. CA-11 (Waterworth) at 66, fn. 108.

<sup>49</sup> See *supra*, Section IV.A.1 at 9:7-20.

1 developed using the 2022 data. For these reasons, Cal Advocates' alternate recommendation for 2022  
2 should be disregarded.

3 **B. Smart Meter 2.0 (WP# 218810)**

4 This section of rebuttal testimony supports SDG&E's IT Capital costs for Smart Meter 2.0. The  
5 Smart Meter 2.0 project replaces the smart meter network, gas modules and implements a new head-  
6 end solution to prevent mass failure of devices and to maintain metering operations at the current high  
7 level.<sup>50</sup> The business justification for this project is described in the Customer Service Field Operations  
8 (CSFO) direct and rebuttal testimonies.<sup>51</sup>

9 SDG&E's IT Capital forecast expenditure for Smart Meter (SM) 2.0 project for 2022, 2023, and  
10 2024 are \$4.292 million, \$32.802 million, and \$58.459 million, respectively.

11 The table below compares the disputed Capital Project Cost for Smart Meter 2.0. to Intervenor's  
12 recommendations.

13 **TABLE BG-WE – 2**  
14 **Comparison of SDG&E and Intervenor**  
15 **Estimated SM 2.0 IT Capital Expenses**

<b>SM2.0 IT CAPITAL – Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	4,292	32,802	58,459	95,553	0
CAL ADVOCATES	2,146	16,401	29,229	47,776	(47,777)
TURN	0	0	0	0	(95,553)
UCAN	4,292	32,802	0	37,094	(58,459)

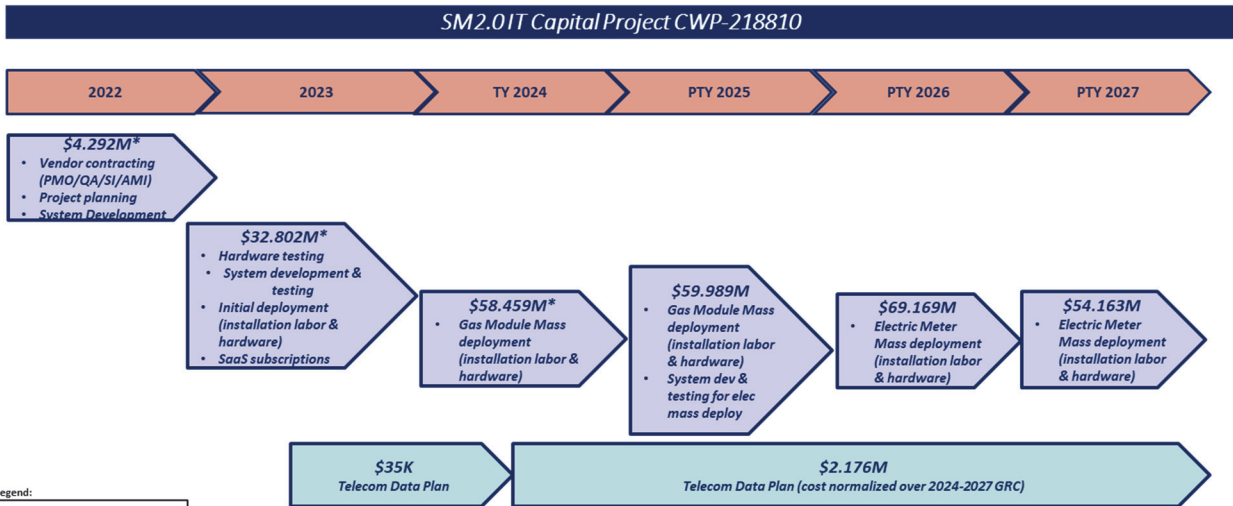
16 SDG&E provides the following Gantt chart in Figure BG-WE-2 to depict the critical milestones  
17 with forecasted spend by year and a high-level schedule of the work to be completed for SM 2.0.

<sup>50</sup> Ex. SDG&E-25-CWP-R (Information Technology) at 71.

<sup>51</sup> Ex. SDG&E-17-R (Revised Prepared Testimony of David Thai (Customer Services – Field Operations)); Ex. SDG&E-217 (Rebuttal Testimony of David Thai (Customer Services – Field Operations)).

1  
2

**Figure BG-WE – 2**  
**SMART METER 2.0 IT CAPITAL PROJECT (CWP 218810)<sup>52</sup>**



Legend:  
■ Capital  
■ O&M (IT O&M Related to SM2.0 ONLY)

\*Source: Ex. SDG&E-25-CWP/Witness W.Exon page 71-79 of 823

3  
4  
5

### 1. CAL ADVOCATES

6  
7  
8  
9  
10

Cal Advocates proposes funding SM 2.0 IT Capital project at 50% of SDG&E’s Capital forecast.<sup>53</sup> This results in a reduction of \$2.146 million in 2022, \$16.401 million in 2023, and \$29.230 million in 2024. “Cal Advocates does not take issue with SDG&E’s justification for the current meter replacement initiative,” but questioned SDG&E’s cost support for the project and “proposes to moderate the level of funding requested by SDG&E.”<sup>54</sup>

11  
12  
13

SDG&E disagrees with Cal Advocates proposal to arbitrarily reduce the level of funding requested by SDG&E, which is at odds with its statement that Cal Advocates recognizes the need for the current meter replacement initiative.

14  
15  
16  
17  
18

Cal Advocates proposal to reduce SM 2.0 capital funding by half would force SDG&E to prioritize the funding from the multi-year program as depicted in Figure BG-WE-2, and only allow the Company to invest and implement the technology foundations for the SM 2.0 program in 2022 and 2023, without the ability to invest in the deployment of the new gas modules and electric meters. This would be equivalent to building a new house, and only have enough funds to lay the slab foundation,

<sup>52</sup> Smart Meter 2.0 PTY 2025-2027 costs (see Ex. SDG&E-17-R (Thai) at DHT-44 (Table DHT-31)); Telecom Data Plan costs (Ex. SDG&E-25-WP (Ballard) at 46-50 (Section 2100-0207.000 - Shared Operational Infrastructure)).

<sup>53</sup> Ex. CA-10 (Campbell) 34:27-28.

<sup>54</sup> Ex. CA-10 (Campbell) 34:21-22, 34:26-27.

1 but no funds to build the house structure on top of the slab foundation. The result is an incomplete  
2 project that does not fully meet the original requirements and may not provide the desired benefits and  
3 outcomes.

4 If the Commission were to adopt Cal Advocates' proposed 50% disallowance, it may lead to  
5 delayed and/or deferred deployment of gas modules and electric meters, resulting in higher costs  
6 reacting to meter failures, which will harm rate payers. SDG&E requests that the Commission reject  
7 Cal Advocates recommendation of 50% reduction and adopt SDG&E's forecast in its entirety as  
8 reasonable.

## 9 2. TURN

10 TURN recommends rejecting the entirety of SDG&E's SM 2.0 IT Capital requests in 2022,  
11 2023, and 2024 of \$4.292 million, \$32.802 million, and \$58.459 million, respectively.

12 TURN states that SDG&E has not met the burden of proof for the funding of the SM 2.0 IT  
13 Capital forecast. SDG&E disagrees. The direct and rebuttal CSFO testimonies (Ex. SDG&E-17-R and  
14 SDG&E-217) describe the business need and justification for the SM 2.0 project. SDG&E's response to  
15 TURN-SEU-052 provided ample and robust support for this project. Smart Meter 2.0 program details  
16 provided to TURN included:

- 17 • Smart Meter 2.0 Update (September 10, 2021) report providing the project  
18 status, scope, estimated costs and schedule.
- 19 • Smart Meter 2.0 Executive Presentation (March 11, 2022, and April 6, 2022)  
20 seeking approval of the AMI Technology vendor recommendation. Topics  
21 included vendor analysis, project scope, schedule, costs, and benefits.
- 22 • Portfolio Governance Committee (PGC) Meeting (March 23, 2022) provided  
23 financial update, detailed financials, and revised timeline.
- 24 • Work Order Authorization -WOA (March 30, 2022) granting approval and  
25 budget for the project.

26 Contrary to TURN's assertion, SDG&E conducts a rigorous process and vetting before moving  
27 forward with any major IT investment, such as SM 2.0. That process includes the development of a  
28 business case and analysis of the need and costs for a particular project.<sup>55</sup> If the Commission were to

---

<sup>55</sup> Ex. SDG&E-25 (Information Technology) at TLB/WJE-22. See Appendix D, at BG-WE-D-1 (Illustration of IT Project Lifecycle as part of SDG&E Response to DR PAO-SDGE-043-LMW, Question 1.e.)

1 adopt TURN’s recommendation to deny funding for this project, SDG&E will not be able to invest in  
2 the required technology foundations to meet the business operations’ need for deployment of new gas  
3 modules and electric meters. The impacts of not funding the Smart Meter 2.0 project are described in  
4 the direct and rebuttal CSFO testimonies. SDG&E requests that the Commission reject TURN’s  
5 recommendation and adopt SDG&E’s forecast in its entirety as reasonable.

### 6 3. UCAN

7 UCAN recommends disallowing SDG&E’s 2024 SM 2.0 IT Capital forecast request for  
8 \$58.459 million.<sup>56</sup> UCAN did not address capital project costs in 2022 and 2023. UCAN claims that  
9 SDG&E’s technology projects should be disallowed because they “look to be either obsolete or at best  
10 ‘interim’ (useful for two years or less) in the life cycle of smart grid requirements.”<sup>57</sup> Included within  
11 the “specific list of IT assets that [UCAN claims] will be outmoded, obsolete, and stranded within this  
12 GRC period are” Smart Meter 2.0.<sup>58</sup> UCAN is incorrect, as described above in my discussion in  
13 Section III.A addressing UCAN’s assertions about technology obsolescence. UCAN provides no  
14 factual basis to support its assertion that the SM 2.0 technology will be obsolete or interim within the  
15 TY 2024 GRC cycle and should be disregarded.

16 Even then, UCAN proposes only to disallow funding in 2024. This proposal would force  
17 SDG&E to prioritize the funding and only allow SDG&E to invest and implement the technology  
18 foundations for the SM 2.0 program in 2022 and 2023, without the ability to invest in the deployment  
19 of the new gas modules and electric meters. Additionally, if the disallowance is adopted for 2024, it  
20 may lead to delayed and/or deferred deployment of gas modules and electric meters, resulting in higher  
21 costs as replacements must continuously be sourced to address meter failures, to the detriment of rate  
22 payers.

23 If the Commission were to adopt UCAN’s recommended 2024 disallowance, SDG&E will not  
24 be able to meet the business operations need to procure and deploy the new gas modules and electric  
25 meters. The impacts of not funding the Smart Meter 2.0 project are described in the direct and rebuttal  
26 CSFO testimonies. SDG&E requests that the Commission reject UCAN’s recommendation and adopt  
27 SDG&E’s forecast as reasonable.

---

<sup>56</sup> Ex. UCAN (Woychik) at 280.

<sup>57</sup> *Id.* at 280.

<sup>58</sup> *Id.*

**C. Smart Meter Product/Upgrade – (WP# 00900D & WP# 00900E)**

This section of rebuttal testimony supports SDG&E’s IT Capital costs for Smart Meter Product/Upgrade project. The business justification for this project is sponsored in the direct and rebuttal testimony of CSFO (Ex. SDG&E-17-R and SDG&E-217).

SDG&E’s IT Capital forecast expenditure for the Smart Meter Product/Upgrade project for 2022, 2023, and 2024 are \$5.141 million, \$6.208 million, and \$3.663 million, respectively.

The table below compares the disputed IT Capital Project Cost for Smart Meter Product/Upgrade.

**TABLE BG-WE – 3  
Comparison of SDG&E and Intervenors  
Estimated Smart Meter Product/Upgrade IT Capital Expenses**

<b>Smart Meter Product/Upgrade IT CAPITAL – Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	5,141	6,208	3,663	15,012	0
CAL ADVOCATES <sup>59</sup>	5,141	5,141	0	10,282	(4,730)
TURN	5,141	6,208	3,663	15,012	0
UCAN	5,141	6,208	0	11,349	(3,663)

The SDG&E Smart Meter systems are a critical set of applications that configure, collect, manage, and validate data from meters for Billing, Load Research, Outage Management, Customer On-Line Presentment, and many other operational processes. The set of applications [Meter Data Management System (MDMS), Openway Collection Engine (OWCE), Certicom, and MV90] were last upgraded in 2017 (MV90 upgraded in 2019). Since that time, platform and software versions have advanced to the point whereby all current versions are either past or nearing end-of-support by the manufacturer. Upgrading to supported operating and database platforms is necessary as vendors stop providing support or security updates, also known as technical debt, requiring application software upgrades.

The risk of not performing the upgrade is that SDG&E would be left with technology obsolescence by way of unsupported operating system, database, and Itron application versions. This is

<sup>59</sup> As described in Section V, Sub-Section A, Cal Advocates recommends two contradictory positions in its testimony (*See* Ex. CA-10 (Campbell) and Ex. CA-11 (Waterworth)) for the Smart Meter Product/Upgrade forecast. Cal Advocates’ recommendation at page 67, Table 11-34 of Exhibit CA-11 states no funding, which contradicts the recommendation for reduced funding at page 33, Table 10-23 of Exhibit CA-10. To reflect a comparison between Cal Advocates and SDG&E’s forecasts, SDG&E used the source data at page 33, Table 10-23 of Exhibit CA-10 as Cal Advocates Capital recommendation for Smart Meter Product/Upgrade.

1 an issue because SDG&E would no longer receive critical security and software patches from our  
 2 vendors; and our vendors would have no obligation to support SDG&E in resolving any issues.  
 3 Without necessary support and updates, our systems would become incompatible with other systems on  
 4 different versions of operating systems & database platforms.

5 Additionally, these critical applications become increasingly vulnerable to cybersecurity  
 6 threats. Upgrades to both Operating system and application versions are required to leverage the  
 7 latest encryption algorithms such as Transport Layer Security (TLS 1.2).

8 The table below depicts planned updates and on-going activities the Smart Meter Product Team  
 9 plans to accomplish each year. SDG&E makes the distinction between a Product team and a Project  
 10 team. A Product team is responsible for the ongoing development and improvement of a particular  
 11 product, while a Project team is focused on delivering a specific set of goals within a defined  
 12 timeframe. In a product-centric model, Product teams are composed with cross-functional participants  
 13 and members with diverse skillsets that work together towards common goals. For example, Product  
 14 teams are tasked with prioritizing system enhancements that provide value in terms of operational  
 15 efficiency, reliability, compliance, and customer satisfaction. SDG&E supports the fact that Product  
 16 teams play a critical role in identifying new technologies, performing technology updates, and  
 17 addressing system vulnerabilities that help mitigate technology obsolescence.

18 **Table BG-WE – 4**

Team	Feature/Enhancement	2022	2023	2024
Smart Meter Product	Meter Deregistration Automation		X	
Smart Meter Product	Field Area Router Business Operation Enhancements		X	
Smart Meter Product	MV 90 Upgrade			X
Smart Meter Product	Enhancement of Centralized Operations Key Performance Indicators (KPI) & Exception (COKE) and Datamart to support improved reliability, security, and performance		X	X
Smart Meter Product	Enhancement of Customer Energy Network (CEN) to support improved reliability, security, and performance		X	X
Smart Meter Product	Migration of Meter Shop Watthour Engineering Co. (WECO) database to improve security, reliability, and performance of the operational database		X	

Team	Feature/Enhancement	2022	2023	2024
Smart Meter Product	Automated testing of all new code to the COKE and Datamart applications to reduce manual work		X	X
Smart Meter Product	Creation and enhancements of automated reports that will track the reliability and performance of the Advanced Metering Infrastructure (AMI) system and Smart Meter 2.0		X	X
Smart Meter Product	Creation and enhancement of automated reports that will identify non-communicating gas meters to supported improved reliability		X	
Smart Meter Product	Upgrades of software and servers to support enhanced security and improve performance by remediating redundant software		X	
Smart Meter Product	Creation and enhancement of automated reports that measure KPI's of AMI operational and billing metrics		X	
Smart Meter Product	Development of automated network stabilization application and webservice that will reduce manual work associated with AMI meter changes			X
Smart Meter Product	Creation and development of application that will monitor and report on the reliability and lifecycle of AMI hardware which will reduce manual work and improve reporting on meter performance			X
Smart Meter Upgrade (Production and Non-Production)	What's Up Gold (Network Monitoring Application) – Upgrades of application software version, servers, and database to support enhanced cyber security and performance.	X		
Smart Meter Upgrade (Production and Non-Production)	Certicom – Encryption and Encryption Key Server – Upgrades of application software version, servers, and database to support enhanced cyber security and performance.	X	X	
Smart Meter Upgrade (Production and Non-Production)	OpenWay Collection Engine (OWCE) – Upgrades of application software, servers, and database to support enhanced cyber security and performance.	X		
Smart Meter Upgrade (Production and Non-Production)	Meter Data Management System (MDMS) – Upgrades of application software version, servers, and		X	X



Team	Feature/Enhancement	2022	2023	2024
	database to support enhanced cyber security and performance.			
Smart Meter Upgrade (Production and Non-Production)	Implement Test Automation for OWCE and MDMS to enhance the reliability of the application software.	X	X	X

1                   **1. Cal Advocates**

2                   Cal Advocates does not oppose SDG&E’s 2022 forecast of \$5.141 million. Cal Advocates  
3 recommends a reduction of \$1.067 million for 2023 from \$6.208 million to \$5.141 million. Cal  
4 Advocates recommends no funding for year 2024, equating to a disallowance of \$3.663 million. Cal  
5 Advocates takes issue with the Smart Meter Product/Upgrade justification. Cal Advocates states “the  
6 business rationale of Smart Meter Product/Upgrade is unjustified.”<sup>60</sup>

7                   SDG&E disagrees with the Cal Advocates recommendation to severely reduce the scope of the  
8 Smart Meter Product/Upgrade and disagrees that it has not met the burden of proof supporting the IT  
9 Capital funding of Smart Meter Product/Upgrade. SDG&E reiterates that it presents a full and complete  
10 description of the business justification and customer benefit that will accrue from this project in the  
11 direct and rebuttal CSFO testimonies (Exhibits SDG&E-17-R and SDG&E-217). In addition, SDG&E  
12 has compiled in Table BG-WE – 4 above, a list of the Smart Meter Product/Upgrade features and  
13 enhancements being implemented in 2022, 2023, and 2024. And as stated above in Section V, Sub-  
14 Section C, a Product team is responsible for the ongoing development and improvement of a particular  
15 product, while a Project team is focused on delivering a specific set of goals within a defined  
16 timeframe. Cal Advocates fails to recognize the significant operational risks associated with the  
17 disallowance of funding such a critical Product Team that is needed to define the product roadmap, and  
18 manage the product’s development and delivery. The lack of dedicated Product Team engagement and  
19 oversight could lead to costly mistakes, missed opportunities, inefficient allocation of resources, delays,  
20 and failure to deliver features and enhancements that are critical for business success.

21                   If the Commission were to adopt Cal Advocates forecast, SDG&E will not be able to fully  
22 engage and sustain the Product Team in addressing the enhancement and upgrade needs, resulting in  
23 not being able to remediate known cybersecurity and technology obsolescence risks, as well as not

---

<sup>60</sup> Ex. CA-10 (Campbell) 37:17-18.

1 being able to report on meter failures resulting in potential impacts to customer bills. SDG&E requests  
2 the Commission to reject Cal Advocates position and adopt SDG&E’s forecast as reasonable.

## 3 2. UCAN

4 UCAN recommends rejecting SDG&E’s Smart Meter Product/Upgrade project 2024 IT Capital  
5 request of \$3.663 million. UCAN did not address capital project costs in 2022 and 2023. UCAN takes  
6 issue with capital forecast for Smart Meter Product/Upgrade and states that “these capital costs are not  
7 justified”<sup>61</sup> in addition to raising obsolescence, as it did with the SM 2.0 project above.<sup>62</sup>

8 SDG&E disagrees with UCAN’s position and has addressed the issue of technological  
9 obsolescence in Section III, Sub-Section A. SDG&E disagrees with UCAN’s unsupported claims that  
10 the costs are not justified or subject to short-term obsolescence.

11 In addition to the project details contained in direct testimony and workpapers (Ex. SDG&E-25  
12 and SDG&E-25-CWP), SDG&E provided Smart Meter Product/Upgrade details in response to  
13 discovery.<sup>63</sup> These materials included:

- 14 • Portfolio Governance Committee (PGC) Meeting (November 17, 2021) provided  
15 financial update, detailed financials and revised timeline and received project  
16 approval.
- 17 • Work Order Authorization -WOA (January 1, 2022) granting approval and  
18 budget for the project.
- 19 • Portfolio Governance Committee (PGC) Meeting/Off Cycle Approval  
20 (August 24, 2022) report providing the revised project status, scope, estimated  
21 costs and schedule.

22 A thorough description of the business justification that will accrue from this project is also  
23 contained in the direct and rebuttal CSFO testimonies (Exhibits SDG&E-17-R and SDG&E-217). In  
24 addition, SDG&E has compiled in Table BG-WE-4 above, a list of the Smart Meter Product/Upgrade  
25 features and enhancements being implemented in 2022, 2023, and has described the importance and  
26 value of Product Teams in Section V, Sub-Section C.

---

<sup>61</sup> Ex. UCAN (Woychik), page 14:17-21.

<sup>62</sup> *See id.* at 280.

<sup>63</sup> *See, e.g.*, SDG&E Response to TURN-SEU-052 dated March 31, 2023.

SDG&E reiterates that there are significant operational risks associated with the disallowance of 2024 funding for the Product Team. SDG&E will not be able to engage the Product Team to address the updates, resulting in not being able to remediate known cybersecurity and technology obsolescence risks, as well as not being able to report on meter failures resulting in potential impacts to customer bills. SDG&E requests that the Commission to reject UCAN’s position and adopt SDG&E’s forecast as reasonable.

**D. Field Service Delivery (FSD) (RAMP) – (WP# 00920AI & WP# 00920T)**

This section of rebuttal testimony supports SDG&E’s IT Capital costs for FSD. The business justification for this project is described in the CSFO direct and rebuttal testimonies of (Exhibits SDG&E-17-R and SDG&E-217).

SDG&E’s IT Capital forecast expenditure for the Field Service Delivery (FSD) project for 2022, 2023, and 2024 are \$13.400 million, \$13.839 million, and \$19.296 million, respectively.

FSD is a critical system that distributes electric and gas distribution work packages to the field. This system is critical for operations to complete their daily work. SDG&E’s current FSD system is ClickSoftware version 8.1, and it was originally deployed into production over 10 years ago. In 2019, Salesforce acquired Click and announced the end of life for the ClickSoftware on-site version with sustaining support ending on December 31, 2020. Salesforce is requiring all ClickSoftware on-site customers to move to their Salesforce Cloud version. Currently, we have limited support from Salesforce for security and bug fixes, which poses significant risk in meeting the changing business requirements and/or keeping the software secure.

The table below illustrates the disputed IT Capital Project Cost for FSD.

**TABLE BG-WE – 5  
Comparison of SDG&E and Intervenors  
Estimated FSD IT Capital Expenses**

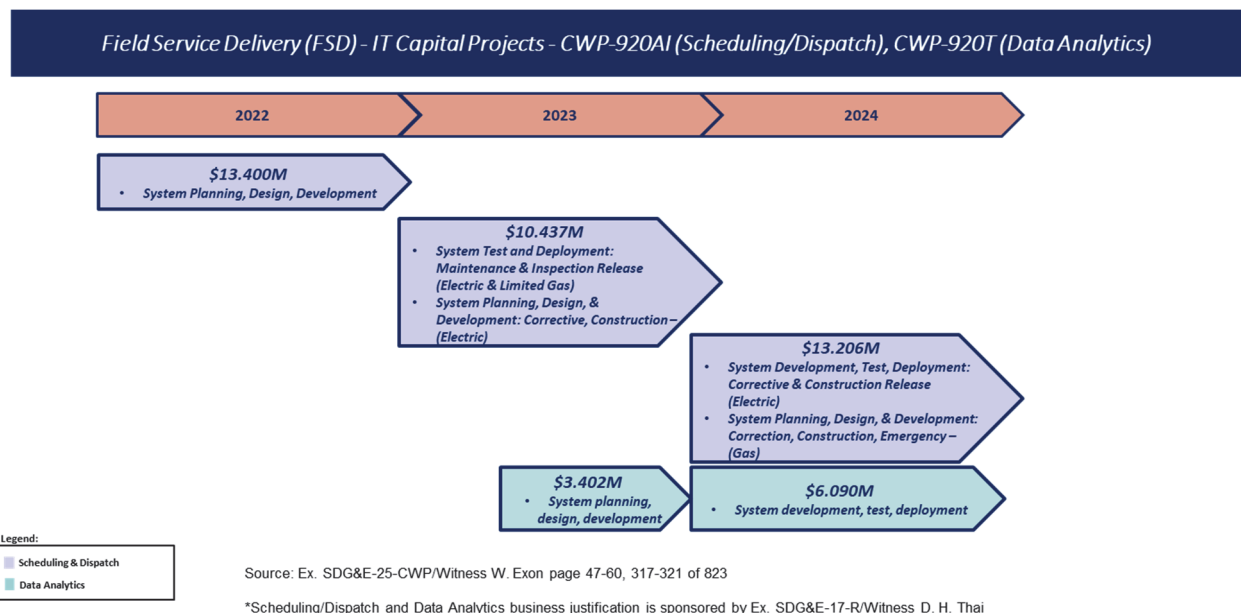
<b>FSD IT CAPITAL – Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	13,400	13,839	19,296	46,535	0
CAL ADVOCATES <sup>64</sup>	13,400	13,400	13,400	40,200	(6,335)

<sup>64</sup> As described in Section V, Sub-Section A, Cal Advocates recommends contradictory positions regarding the FSD forecast in its two testimonies (*See Ex. CA-10 (Campbell) and Ex. CA-11 (Waterworth)*). Cal Advocates recommendation at page 67, Table 11-34 of Exhibit CA-11 recommends no funding, which contradicts the recommendation for reduced funding at page 33, Table 10-23 of Exhibit CA-10. To reflect a comparison between Cal Advocates and SDG&E’S FSD forecast, SDG&E used the source data at page 33, Table 10-23 of Exhibit CA-10 as Cal Advocates Capital recommendation for FSD.

FSD IT CAPITAL – Constant 2021 (\$000)					
	2022	2023	2024	Total	Difference
TURN	0	0	0	0	(46,535)
UCAN	13,400	13,839	0	27,239	(19,296)

SDG&E provides the following Gantt chart in Figure BG-WE-3 to depict the critical milestones with forecasted spend by year and a high-level schedule of the work to be completed for FSD.

**Figure BG-WE – 3**  
**FSD IT CAPITAL PROJECT (CWP 920AI & 920T)**



## 1. CAL ADVOCATES

Cal Advocates does not oppose SDG&E’s 2022 forecast for \$13.400 million. Cal Advocates recommends a reduction of \$0.439 million for 2023 from \$13.839 million to \$13.400 million. Cal Advocates recommends a reduction of \$5.896 million for 2024 from \$19.296 million to \$13.400 million. Cal Advocates states “SDG&E data request response do not support the funding request of \$13.400 million for 2022, \$13.839 million for 2023, and \$19.296 million for 2024 for this capital project.”<sup>65</sup>

SDG&E disagrees with Cal Advocates recommended disallowances and its claim that SDG&E has failed to provide sufficient program justification. The multi-year program as depicted in Figure BG-WE-3 above will implement an integrated, cohesive, and modern technology solution for field

<sup>65</sup> Ex. CA-10 (Campbell) at 36:29-30.

1 operations and supporting business organizations. In addition to details in testimony and workpapers  
2 (SDG&E-25 and SDG&E-CWP-R), SDG&E provided FSD program details in discovery that included  
3 copies of business case approval, work order authorization approval, project submission in portfolio  
4 management tool, and FSD program overview as described below.

5 If the Commission were to adopt Cal Advocates' recommendation, SDG&E will be unable to  
6 implement FSD as planned, resulting in implementation delays, higher costs, risk of continued  
7 technology obsolescence, potential stranded assets, increased risk of cybersecurity threats, that would  
8 lead to an inability to achieve customer and operational benefits. SDG&E requests the Commission to  
9 reject Cal Advocate's recommendations and adopt SDG&E's forecast as reasonable to avoid the risk of  
10 maintaining an unsupported software product.

## 11 2. TURN

12 TURN recommends rejecting SDG&E's FSD IT capital project forecast in 2022, 2023, and  
13 2024 in its entirety of \$13.400 million, \$13.839 million, and \$19.296 million, respectively. TURN  
14 asserts that "SDG&E has failed to provide clear and convincing evidence for why such spending would  
15 result in just and reasonable rates."<sup>66</sup>

16 SDG&E disagrees with TURN regarding SDG&E failing to meet the burden of proof for the  
17 funding of FSD. In addition to the description of this project and its need in testimony and workpapers,  
18 TURN received in discovery FSD program details that included:

- 19 • FSD Executive Business Case Update (June 4, 2020) report providing the project  
20 strategy, benefits, high level scope, and estimated costs.
- 21 • Portfolio Governance Committee (PGC) Meeting (July 15, 2020) provided  
22 financial update, detailed financials, and timeline.
- 23 • Work Order Authorization -WOA (August 17, 2020) granting approval and  
24 budget for the project.

25 If TURN's recommendation was adopted, SDG&E would be unable to implement an integrated,  
26 cohesive, and modern technology solution for field operations and supporting business organizations,  
27 which has already commenced preparations for the project. In 2022, the FSD Product Team gathered  
28 business and technical requirements and completed the RFP process and selected a software vendor for  
29 the forecasting, scheduling and dispatch solution. In 2023, SDG&E has been working on the design,

---

<sup>66</sup> Ex. TURN-09 (Cheng) at 26:12-13.

1 development and testing for the new FSD system. If the Commission were to adopt TURN's  
2 recommendation, SDG&E will be unable to implement the remainder of the year 2023 and 2024 project  
3 tasks and potentially could leave a stranded asset and will increase the risk of cybersecurity threats and  
4 technology obsolescence. Ultimately, the inability to replace the existing FSD system could pose a risk  
5 communicating instructions to SDG&E field crews, which could cause delays in such things as  
6 maintenance activities, as further described in the direct and rebuttal CSFO testimonies (Exhibits  
7 SDG&E-17-R and SDG&E-217).

8 SDG&E requests the Commission to reject TURN's recommendation and adopt SDG&E's  
9 forecast to execute updates to software as necessary and reasonable.

### 10 3. UCAN

11 UCAN recommends rejecting SDG&E's FSD project Capital request in 2024 for \$19.296  
12 million. UCAN did not address capital project forecast costs in 2022 and 2023. UCAN states that  
13 "SDG&E fails to provide adequate justification to demonstrate that these should be included in  
14 customer rates."<sup>67</sup> UCAN further claims that SDG&E's existing FSD is obsolete and SDG&E's  
15 proposed FSD project "would finance a platform that will soon be obsolete and outmoded [and] are not  
16 economically justified. . . ."<sup>68</sup> SDG&E disagrees with UCAN's position and has addressed the issue of  
17 technological obsolescence in Section III, Sub-Section A. In addition to the description provided  
18 above, and in its direct testimony and workpapers for this project (Ex. SDG&E-25 and SDG&E-25-  
19 CWP-R), SDG&E presents the business justification and customer benefit that will accrue from this  
20 project in the direct and rebuttal CSFO testimonies (Exhibits SDG&E-17-R and SDG&E-217). Absent  
21 the TY 2024 funding as UCAN recommends, SDG&E will not be able to complete the technology  
22 implementation and will be unable to realize the full benefits, resulting in higher costs and potential  
23 stranded assets, and the risk to customers as described in the direct and rebuttal CSFO testimonies.

24 As discussed above, SDG&E has already begun preparations for the implementation of this  
25 project by gathering business and technical requirements, conducting an RFP and selecting a software  
26 vendor for the forecasting, scheduling and dispatch solution. In 2023, SDG&E began working on the  
27 design, development and testing for the new FSD system. If the Commission were to adopt UCAN's  
28 recommendation, SDG&E will not be able to fully complete the implementation of the new FSD

---

<sup>67</sup> Ex. UCAN (Woychik) at 300:10-13.

<sup>68</sup> *Id.*

1 system and continuing to use an unsupported system that will limit functionality and cause significant  
 2 gaps in operational capabilities and risks to effectively communicate instructions to the field crews.  
 3 Failure to fund this project would subject SDG&E and its customers to rely on an unsupported system  
 4 and without the ability to adapt and meet changing business environments. SDG&E requests that the  
 5 Commission reject UCAN’s recommendation that would impede the Company’s ability to  
 6 communicate with field crews and find SDG&E’s forecast as reasonable.

7 **E. Field Mobility Development (WP# 00920AS)**

8 This section of rebuttal testimony supports SDG&E’s IT Capital costs for Field Mobility  
 9 Development. The business justification for this project is described in the direct and rebuttal  
 10 testimonies of Safety, Risk & Asset Management Systems (Ex. SDG&E-31-R and SDG&E-231).

11 The table below illustrates the disputed IT Capital Project Cost for Field Mobility Development.

12 **TABLE BG-WE – 6**  
 13 **Comparison of SDG&E and Intervenors**  
 14 **Estimated Field Mobility Development IT Capital Expenses**

<b>FIELD MOBILITY DEVELOPMENT IT CAPITAL – Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	1,835	0	0	1,835	0
CAL ADVOCATES	1,835	0	0	1,835	0
TURN	1,835	0	0	1,835	0
UCAN	1,835	0	0 <sup>69</sup>	1,835	0

15 SDG&E’s IT Capital forecast expenditure for the Field Mobility Development project for 2022,  
 16 2023, and 2024 are \$1.835 million, \$0, and \$0, respectively.

17 **1. UCAN**

18 UCAN does not address SDG&E’s 2022 or 2023 IT Capital forecast but recommends that the  
 19 Commission reject SDG&E’s Field Mobility Development project IT Capital forecasted costs for Test  
 20 Year 2024.<sup>70</sup>

21 UCAN states that “SDG&E has only provided a cursory justification for these projects and  
 22 provides no assurances that these projects will avoid technological obsolescence.”<sup>71</sup> While UCAN takes

<sup>69</sup> Although SDG&E is not forecasting any costs in the Test Year 2024, UCAN has objected to the Test Year forecast.

<sup>70</sup> Ex. UCAN (Woychik) at 300:6-16.

<sup>71</sup> *Id.* at 304:9-10.

1 issue with IT Capital forecast for Field Mobility Development; it fails to note that this project was  
 2 completed in 2022, is in service, is used and useful and that SDG&E has not forecasted IT Capital costs  
 3 beyond 2022. UCAN provides no support for its position on obsolescence for this project. SDG&E  
 4 disagrees with UCAN’s position and has addressed the issue of technological obsolescence in Section  
 5 III, Sub-Section A. The failure to invest in technology to update, maintain or replace technology may  
 6 lead to risks including, but not limited to, unavailability of systems critical to the way SDG&E  
 7 conducts base business. Operating technologies that are unsupported also increase the cyber risk and  
 8 potential unauthorized breaches to systems and customer data. UCAN’s position to reject SDG&E’s  
 9 investment in technology will not only lead to increased risks and cybersecurity threats but will also  
 10 have a direct impact in the delivery of reliable, safe, efficient, and secure services to customers.

11 SDG&E requests that the Commission reject UCAN’s position and adopt SDG&E’s forecast as  
 12 reasonable. No other party objected to this Capital forecast.

13 **F. CIS Regulatory & Enhancements – (WP# 00903E, WP# 00903F, WP# 00903G)**

14 This section of rebuttal testimony supports SDG&E’s IT Capital costs for CIS Regulatory &  
 15 Enhancements. The business justification for this project is described in the direct and Customer  
 16 Services Office Operations (CSOO) rebuttal testimonies (Exhibits SDG&E-18 and SDG&E-218).  
 17 SDG&E’s IT Capital forecast expenditures for the CIS Regulatory & Enhancements projects for 2022,  
 18 2023, and 2024 are \$19.233 million, \$19.752 million, and \$23.768 million, respectively.

19 The table below compares the disputed IT Capital Project Forecast Costs for CIS Regulatory &  
 20 Enhancements.

21 **TABLE BG-WE – 7**  
 22 **Comparison of SDG&E and Intervenors**  
 23 **Estimated CIS Regulatory & Enhancements IT Capital Expenses**

<b>CIS REGULATORY &amp; ENHACEMENTS IT CAPITAL - Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	19,233	19,752	23,768	62,753	-
CAL ADVOCATES	19,233	19,752	23,768	62,753	-
TURN	0	0	0	0	(62,753)
UCAN	19,233	19,752	0	38,985	(23,768)

24 The tables below include list the scope of enhancements that are planned and on-going that have  
 25 been identified and/or implemented since the 2021 CIS go-live date.  
 26



**Table BG-WE – 8  
CIS Regulatory & Enhancements 2022**

Enhancement	Category			
	Customer Transition to CCA	Regulatory and Compliance	Self Service and Security	Business Operations / Automation
Enhancements to existing CCA reports to capture additional customer attribute data.	X			X
System changes and performance testing to support 2022 CCA Transition	X			
System changes to support the transition for customers on the Levelized Pay Program, enabling settlement balances to transfer with the transition and incorporate CCA billing charges.	X	X		X
CCA Payment Allocation and Financial Reporting to support additional requirements from the CCAs.	X			X
System changes to SDG&E's MyAccount platform to incorporate requested billing charge detail and messaging for Community Choice Aggregation.	X	X	X	
California Arrearage Payment Program (CAPP): implemented new programs to apply two rounds of payments (2022, 2023) for eligible customers in need of debt relief.		X		X
Enhancements and monitoring to further support 24-month payment plans		X		X
“Two-Factor Authentication” within MyAccount to help secure and protect customer information.			X	
System changes in SDG&E's Interactive Voice Response (IVR) to tailor information to a specific customer to better meet their needs and streamline customer inquiries.	X	X	X	X

MyAccount security enhancements and monitoring			X	
System testing and validations to support SDG&E 2022 SAP Product Upgrades.			X	X

1  
2  
3

**Table BG-WE – 9  
CIS Regulatory & Enhancements 2023**

Enhancement	Category			
	Customer Transition to CCAs	Regulatory and Compliance	Self Service and Security	Business Operations / Automation
A new capability to extract near-real time customer usage data requested by the CCAs, as referenced in Real Time Pricing proceeding.	X	X		X
System changes and performance testing to support 2023 CCA Transition	X			
System changes to SDG&E’s MyAccount platform to incorporate requested billing charge detail and messaging for Community Choice Aggregation.	X	X	X	
Changes to support the Building Decarbonization Order Information Record (OIR), requiring collection and reporting of customer space and water heating information.		X	X	X
Changes to support the CPUC authorized un-tiered TOU-ELEC rate option for customers, which required configuration within SDG&E’s billing system and MyAccount platform.		X	X	
System changes to support an acceleration of the gas and electric Climate Credit distribution to residential and small business customers, as was authorized under D.23.02-014.		X	X	X

Enhancement	Category			
	Customer Transition to CCAs	Regulatory and Compliance	Self Service and Security	Business Operations / Automation
Collections Resumption system changes to support the recent CPUC Decision requiring additional program offerings, messaging, and corresponding compliance reporting for collections activities		X	X	X
Enhancements to SDG&E's customer survey process to account for new programs and tailor to the customer's specific transactions, allowing SDG&E to obtain direct customer feedback that drives continuous improvement efforts.				X
System testing and validations to support SDG&E 2023 SAP Product Upgrades.			X	X
MyAccount security enhancements and monitoring.			X	
Automation of Sarbanes-Oxley (SOX) testing processes to ensure overall compliance of business controls.			X	X
System enhancements to improve MyAccount functionality for residential and small business customers (CCA, bill-to-date/forecast, conditional messaging).	X		X	X
Changes to implement the Modified Cost Allocation Mechanism (MCAM) as authorized under D.19-11-016.		X		
Enhancements to SDG&E's service order process to ensure field employees are provided real-time information about the jobs and customers they are supporting				X

1  
2

**Table BG-WE – 10  
CIS Regulatory & Enhancements 2024**

Enhancement	Category			
	Customer Transition to CCAs	Regulatory and Compliance	Self Service and Security	Business Operations / Automation
System changes and performance testing to support 2024 CCA Transition	X			
System enhancements to provide additional notification capabilities for customers based upon their communication preferences.			X	X
System enhancements to help reduce back-office handle time for work item exceptions.				X
Changes to help improve overall transaction speed for SDG&E MyAccount.			X	
Changes to monitor and support the Modified Cost Allocation Mechanism (MCAM) as authorized under D.19-11-016.		X		
Changes to enhance Rate Comparison capabilities for SDG&E MyAccount and back-office processes.			X	X
Implementation of customer self-service dashboards for medium and large Commercial & Industrial (C&I) customers.			X	X
Continued enhancements to SDG&E’s customer survey process to account for new programs and tailor to the customer’s specific transactions, allowing SDG&E to obtain direct customer feedback that drives				X

Enhancement	Category			
	Customer Transition to CCAs	Regulatory and Compliance	Self Service and Security	Business Operations / Automation
continuous improvement efforts.				
MyAccount security enhancements and monitoring.			X	
System testing and validations to support SDG&E 2024 SAP Product Upgrades.			X	X
Continued enhancements to SDG&E's service order process to ensure field employees are provided real-time information about the jobs and customers they are supporting				X

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14

**1. Cal Advocates**

Cal Advocates reviewed SDG&E’s testimony, workpapers and data request responses and does not oppose the business rationale for the CIS Regulatory and Enhancements capital project. SDG&E has demonstrated that its forecasting assumptions are reasonable and justified. The Commission should adopt SDG&E’s forecast as reasonable.

**2. TURN**

TURN recommends that the CIS Regulatory & Enhancements project be denied in its entirety claiming that SDG&E does not offer adequate justification for the Customer Service System Enhancements and why these functionalities could not have been accomplished as part of the CIS Replacement implementation. TURN further asserts that the benefits for this project sound very similar to the benefits that were supposed to be achieved by the CIS Replacement.<sup>72</sup>

SDG&E disagrees with TURN’s positions and proposed recommendation to not fund the CIS Regulatory & Enhancements project. The importance and justification of this project is detailed in the

---

<sup>72</sup> Ex. TURN-09 (Cheng) at 31-32.

1 direct and rebuttal CSOO testimonies (Ex. SDG&E-18 and SDG&E-218) and is supplemented in  
2 Tables BG-WE-8, BG-WE-9, and BG-WE-10 above, which list the numerous enhancements in scope  
3 to implement within the forecast period. As reflected in the Tables, these enhancements allow the new  
4 CIS to perform new regulatory directives, customer access and security enhancements, and  
5 modifications necessary to support CCA and other customer services, among others, and are  
6 incremental to those contemplated by CIS Replacement project implementation. SDG&E provided  
7 TURN with additional details about this project in discovery, including:

- 8 • Portfolio Governance Committee (PGC) Meeting (December 14, 2022) provided  
9 financial update, detailed financials, and timeline.
- 10 • Work Order Authorization -WOA (January 1, 2022) granting approval and  
11 budget for the project.
- 12 • Work Order Authorization -WOA (January 1, 2023) granting approval and  
13 budget for the project.

14 TURN ignores SDG&E's demonstration of the nature and purpose of this project and the  
15 significant operational and technology risks that would present from a disallowance of funding for this  
16 project. Without authorization for this project, SDG&E would be unable to address new, mandated  
17 regulatory directives and orders, unable to perform system enhancements and upgrades, and, most  
18 importantly, security enhancements — significantly increasing the risk of system compromise,  
19 challenges to prioritize customer needs, define the product roadmap, and manage product development  
20 and delivery. This could lead to costly mistakes, missed opportunities, inefficient allocation of  
21 resources, delays, and failure to deliver enhancements resulting in penalties and/or inability to be out of  
22 regulatory compliance.

23 There is also a risk of stranded assets. In fact, year 2022 CIS Enhancements have been  
24 implemented and are in-service. Similarly, many of year 2023 CIS Enhancements are either completed  
25 or underway. If the Commission were to adopt TURN's recommendation, SDG&E will be unable to  
26 implement the remainder of the year 2023 and 2024 planned enhancements driven by Commission  
27 directives, as identified in Tables BG-WE-9 and BG-WE-10. This will increase the risk of  
28 cybersecurity threats and technology obsolescence. SDG&E requests that the Commission reject  
29 TURN's recommendation and adopt SDG&E's forecast as reasonable.

1                   **3.       UCAN**

2                   UCAN recommends denying the TY 2024 CIS Regulatory & Enhancements project IT Capital  
3 forecast of \$23,768 million and is silent regarding the 2022 and 2023 forecasts. UCAN bases its  
4 recommendation on its position that “IT assets that will be outmoded, obsolete, and stranded within this  
5 GRC period.”<sup>73</sup>

6                   SDG&E disagrees with UCAN’s position and has addressed the issue of technological  
7 obsolescence in Section III, Sub-Section A. UCAN provides no factual evidence to substantiate it’s  
8 position. Technology is by definition prone to obsolescence, which means SDG&E must ensure that its  
9 IT systems are regularly updated and maintained to maximize their lifespan and to properly manage the  
10 risk that systems will eventually become obsolete. The new CIS went live in April 2021 and this CIS  
11 Regulatory & Enhancements project was proposed and designed to implement new regulatory  
12 directives, customer access and security enhancements, and modifications necessary to support CCA  
13 and other customer services, among others, and are incremental to those contemplated by CIS  
14 Replacement project implementation.

15                  If the Commission were to adopt UCAN’s recommendation, SDG&E will be unable to  
16 implement year 2024 planned enhancements driven by Commission mandates, as identified in Table  
17 BG-WE-10. This would result in the risk of being out of compliance, security and/or technology  
18 updates that would increase the risk of cybersecurity threats and technology obsolescence and inability  
19 to deploy any new customer features that would align with future customer strategy. SDG&E requests  
20 that the Commission reject UCAN’s recommendation and adopt SDG&E’s forecast as reasonable.

21                  **G.       Contact Center of the Future (CCotF) – (WP# 00903B)**

22                  This section of rebuttal testimony supports SDG&E’s IT Capital costs for CCotF. The business  
23 justification for this project is sponsored in the direct and rebuttal testimony of Customer Services –  
24 Office Operations (CSOO) (Ex. SDG&E-18 and SDG&E-218).

25                  SDG&E’s Capital forecast expenditure for the Contact Center of the Future (CCotF) project for  
26 2022, 2023, and 2024 are \$0, \$11.285 million, and \$9.789 million, respectively.

27                  This project is a digital transformation of SDG&E’s Customer Contact Center (CCC) that will  
28 move the current technology to a Cloud-hosted environment and leverages artificial intelligence (AI).  
29 The CIS Replacement project did not include the replacement of the systems or enhancements proposed

---

<sup>73</sup> Ex. UCAN (Woychik) at 280:14-15.

1 in the CCotF project. The CIS Replacement project set the foundation to replace the CCC systems and  
 2 help enable the new capabilities from CCotF. CCotF will empower employees with tools to enable a  
 3 customer-centric environment. This project improves customer experience and customer satisfaction  
 4 with enhanced self-service options, such as conversational Interactive Voice Response (IVR), as well as  
 5 increased reliability of Customer Care Center services. CCotF will also enhance the reliability,  
 6 resiliency and security of systems and data which is essential during emergency events. The current  
 7 technologies such as Avaya (voice), Genesys IVR (Interactive Voice Response), and NICE (Workforce  
 8 Management), that SDG&E uses to support its CCC are a decade old and made up of a large stack of  
 9 applications and a variety of systems that have limited capabilities to address customer needs.  
 10 Currently, Genesys on-site solutions are not being enhanced beyond bug fixes and/or security  
 11 updates. Genesys has focused their internal resources on their Cloud product. CCotF is a project that  
 12 will transfer and/or replace many of the CCC legacy systems to a Cloud platform allowing for more  
 13 frequent and quicker updates, modifications, and enhancements to the CCC applications. Avaya, the  
 14 contact center voice system, has filed for Chapter 11 bankruptcy<sup>74</sup> and poses significant risk to keeping  
 15 resilient operations and viability of the product. The customer contact center Cloud platform will  
 16 include “Voice as a Service” and mitigate the risk of Avaya’s viability as a Company and uncertainty.

17 The table below compares the disputed Capital Project Cost for CCotF.

18 **TABLE BG-WE – 11**  
 19 **Comparison of SDG&E and Intervenors**  
 20 **Estimated CCotF IT Capital Expenses**

<b>CCotF IT CAPITAL - Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	0	11,285	9,789	21,074	-
CAL ADVOCATES	0	11,285	9,789	21,074	-
TURN	0	0	0	0	(21,074)
UCAN	0	11,285	0	11,285	(9,789)

21  
 22 The table below illustrates the capabilities that CCotF will deliver in comparison to the current  
 23 legacy custom contact center capabilities.

<sup>74</sup> Reuters, *Avaya files for Chapter 11 bankruptcy*, February 14, 2023, available at:  
<https://www.reuters.com/technology/avaya-files-chapter-11-bankruptcy-2023-02-14/>.



TABLE BG-WE – 12

Capability	Current	CCotF
<b>Intelligent Self Service</b>		
Conversational Interactive Voice Response (IVR)		X
Virtual Assistant		X
Voice to Digital Deflection		X
<b>Orchestration &amp; Routing</b>		
Predictive Intent Detection		X
Enhanced/Intelligent Routing		X
In Queue Experiences and Virtual Hold	X	X
Omni-Channel Contextual Continuity		X
<b>Employee Development</b>		
Remote Worker Experience Manager		X
Knowledge and Content Management	X	X
Next Best Action		X
Training and Coaching	X	X
Real-Time Intent Listening and Script Adherence		X
<b>Advanced Analytics</b>		
Performance Reporting and Dashboards	X	X
Speech and Sentiment Analytics		X
Customer Experience Analytics		X
Predictive Insights		X
Bot Performance Analytics		X
<b>Next-Gen Operations</b>		
Workforce Management	X	X
Automated Quality Monitoring		X
Real-Time Agent Status	X	X
Single Agent Front-End		X
Real-Time Internal Collaboration	X	X
Document Sharing and Co-Browse		X

### 1. Cal Advocates

Cal Advocates reviewed SDG&E's testimony, workpapers and data request responses and does not oppose the business rationale for the Contact Center of the Future capital project. SDG&E has demonstrated that its forecasting assumptions are reasonable and justified. The Commission should adopt SDG&E's forecast as reasonable.

1                                   **2.       TURN**

2                   TURN recommends the CCotF project be denied in its entirety. TURN states that “Given that  
3 the business case is still under development, TURN believes that it is premature for SDG&E to request  
4 funding for the project.”<sup>75</sup>

5                   SDG&E disagrees with TURN’s recommendation and as described above project strategy,  
6 vision, scope, and direct and rebuttal CSOO testimonies (Ex. SDG&E-18 and SDG&E-218) provides  
7 the critical business justification. SDG&E additionally provided TURN with further information in  
8 discovery including, Contact Center Strategy Executive Summary (October 2020) that provided an  
9 overview of the proposed project vision and guiding principles, project scope, and project benefits.  
10 TURN fails to recognize the criticality of this system and its impact to SDG&E’s business operations  
11 and customer service and as well as the significant technology risks associated with the disallowance of  
12 funding such a critical system. SDG&E believes it is reasonable and prudent to perform periodic  
13 modernization of its business capabilities to support the critical obligation to serve customers and this  
14 capital project should be approved. For example, the current Customer Contact Center systems have  
15 nearly reached End-of-Life (EOL) and End-of-Support (EOS) stage, after which time the vendors will  
16 not provide enhancements, security patches, bug fixes and support. The risks associated with  
17 unsupported IT systems is described above in Section III, Sub-Section A, but it is worth repeating again  
18 that there is an increased risk of cyber-attacks when systems go without patches to address newly  
19 identified vulnerabilities and customer service and the customers experience is severely compromised  
20 because intermittent downtime due to aging systems and unplanned incidents can present challenges  
21 taking and responding to customer calls. TURN again fails to understand the criticality of the system  
22 and its impact to SDG&E’s business operations and its customers.

23                   Currently, the SDG&E contact center system is no longer supported by Genesys, which is  
24 requiring its customers to migrate to the Cloud. If the Commission adopts TURN’s recommendation,  
25 SDG&E will default to an aging and unsupported Customer Contact System with limited functionality  
26 and operability, resulting in potentially not being able to meet changing business requirement and  
27 adapting to the increased customer expectations. SDG&E requests that the Commission rejects  
28 TURN’s recommendation and adopt SDG&E’s forecast as reasonable.

---

<sup>75</sup> Ex. TURN-09 (Cheng) at 30:1-3.

1                   **3.       UCAN**

2                   UCAN recommends that the 2024 IT Capital forecast of \$9.789 million be denied but does not  
3 oppose the 2023 forecast IT Capital of \$11.285 million. UCAN states that “IT assets that will be  
4 outmoded, obsolete, and stranded within this GRC period.”<sup>76</sup> yet UCAN presents no evidence that  
5 would suggest this enhanced technology will be obsolete and stranded within the short time frame of  
6 this GRC. SDG&E disagrees with UCAN’s position and has addressed the issue of obsolescence and  
7 the importance of continued maintenance and updating of information technology investments in the  
8 above testimony, Section III, Sub-Section A. SDG&E described the reasons for this project in detail in  
9 its response to TURN-SEU-053.

10                  UCAN offers no alternative for rejecting the 2024 forecast for this project and its lack of an  
11 alternative will default SDG&E into using an obsolete system with limited functionality and services to  
12 SDG&E customers. UCAN does not object to the 2022 and 2023 forecast, and if its recommendation  
13 were adopted, SDG&E will not have an operational Customer Contact Center (CCC) system that is  
14 critical for utilities, especially during emergency situations and to aid in ensuring the safety of  
15 customers. This will have the reverse effect that UCAN claims it wants to avoid and will result in  
16 higher costs, potential stranded assets and will harm ratepayers. For the reasons stated above, SDG&E  
17 requests the Commission reject UCAN’s position and adopt SDG&E’s forecast as reasonable.

18                   **H.       Digital Workspace (RAMP) – (WP# 00908B)**

19                  This section of rebuttal testimony supports both the IT Capital costs and business justification  
20 for this project, as sponsored in the Information Technology direct testimony (Ex. SDG&E-25).  
21 SDG&E’s Capital forecast expenditure for the Digital Workspace project for 2022, 2023, and 2024 are  
22 \$10.694 million, \$0, and \$0, respectively.

---

<sup>76</sup> Ex. UCAN (Woychik) at 280:14-15.

1 The following table illustrates the disputed Capital Project Cost for Digital Workspace.

2 **TABLE BG-WE – 13**  
3 **Comparison of SDG&E and Intervenors**  
4 **Estimated Digital Workspace IT Capital Expenses**

<b>DIGITAL WORKSPACE IT CAPITAL - Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	10,694	0	0	10,694	-
CAL ADVOCATES	10,694	0	0	10,694	-
TURN	10,694	0	0	10,694	-
UCAN	10,694	0	0 <sup>77</sup>	10,694	-

5  
6 **1. UCAN**

7 Only UCAN takes issue with the Capital forecast for Digital Workspace, and then, only the  
8 forecast for 2024. According to UCAN “SDG&E’s capital cost request for SDG&E WP#00908B –  
9 Digital Workspace (RAMP) of \$10.69 million in 2024 and beyond should be denied.”<sup>78</sup> However,  
10 SDG&E only forecasted costs in 2022 for the Digital Workspace project. There is no forecast for 2024  
11 or beyond for this project, which invalidates UCAN’s recommendation.

12 UCAN’s stated concerns are also unjustified. UCAN states that “Thus, instead of ‘reducing  
13 technology obsolescence’ SDG&E may be increasing it with its Digital Workspace proposal.”<sup>79</sup>  
14 SDG&E disagrees with UCAN’s position. The Digital Workplace project replaces older, slower, out of  
15 warranty hardware, with faster, more portable, more secure devices, that can be managed remotely  
16 through a modern desktop management platform, which for the reasons identified in Section III (Sub-  
17 Section A), provide tremendous security, support and operational benefits that address issues created by  
18 obsolescence of the equipment that the Digital Workplace project will replace.

19 The computers that will be replaced in this project are at their current End-of-Life (EOL) and  
20 pose known security risks to our Company data due to old hackable chipsets and the unavailability of  
21 enhanced security features such as fingerprint readers and hidden camera features. There are also risks  
22 caused by unauthorized installations of hardware and software on these older devices that may be  
23 undetected by the Company’s current management platform. If these gaps are not addressed, the risk of

<sup>77</sup> Although SDG&E is not forecasting any costs in the Test Year 2024, UCAN has objected to the Test Year forecast.

<sup>78</sup> Ex. UCAN (Woychik) at 303:6-7.

<sup>79</sup> *Id.* at 302:20-22.

1 a successful cyber-attack is heightened and unnecessarily place SDG&E at risk of severe negative  
2 consequences and outcomes.

3 This investment includes new capabilities such as application-level security controls, multi-  
4 factor authentication, remote break-fix capabilities, remote software updates and the ability to provide a  
5 personalized user experience across client devices. Regardless of time and space, SDG&E's workforce  
6 can access the systems to be productive and support Company operations.

7 This project is replacing end-of-life devices, and the investment is expected to meet the  
8 Company's standard 5–7-year lifecycle for devices of this nature. For SDG&E's business operations to  
9 run smoothly and efficiently, it is essential for the Company to stay current with supported devices and  
10 enhanced capabilities to avoid falling behind industry standards. The Digital Workspace project is a  
11 prudent and necessary technology investment for the Company's ongoing operations and future growth.

12 UCAN also states, "While this project is considered by SDG&E to be included as a RAMP  
13 activity, SDG&E has failed to explain what specific risk mitigations it expects to achieve."<sup>80</sup> UCAN is  
14 incorrect. In my direct testimony,<sup>81</sup> SDG&E has clearly identified the Digital Workspace project  
15 within the End User Access and Supporting Services CFF activity that mitigates safety risks identified  
16 in the 2021 RAMP Report: Foundational Technology Systems (FTS) Chapter CFF-4. According to the  
17 description of RAMP ID "SDG&E-CFF-4-06," the RAMP activity "End User Access and Supporting  
18 Services" is described as "The End User Access and Supporting Services initiative enhances IT systems  
19 and software security by upgrading the tools and technology used for remote access." The Digital  
20 Workspace project directly aligns and supports the RAMP activity by mitigating risks such as,  
21 replacing out of warranty and End-of-Life (EOL) end user devices that are known to pose security risks  
22 to the Company data and assets.

23 For the reasons stated above, SDG&E requests the Commission reject UCAN's position and  
24 adopt SDG&E's forecast as reasonable.

25 **I. Virtual Desktop Infrastructure (VDI) Expansion – Phase 2 (RAMP) – (WP#**  
26 **00908C)**

27 This section of rebuttal testimony supports both the IT Capital costs and business justification  
28 for this project, as sponsored in the Information Technology direct testimony (Ex. SDG&E-25).

---

<sup>80</sup> *Id.* at 303:4-6.

<sup>81</sup> Ex. SDG&E-25 (Information Technology) at TLB/WJE-34.

1 SDG&E’s Capital forecast expenditure for the Virtual Desktop Infrastructure (VDI) Expansion project  
2 for 2022, 2023, and 2024 are \$0, \$1.550 million, and \$1.550 million, respectively.

3 The table below illustrates the disputed Capital Project Cost for VDI Expansion.

4 **TABLE BG-WE – 14**  
5 **Comparison of SDG&E and Intervenors**  
6 **Estimated VDI Expansion IT Capital Expenses**

<b>VDI EXPANSION IT CAPITAL – Constant 2021 (\$000)</b>					
	<b>2022</b>	<b>2023</b>	<b>2024</b>	<b>Total</b>	<b>Difference</b>
SDG&E	0	1,550	1,550	3,100	<b>0</b>
CAL ADVOCATES	0	1,550	1,550	3,100	<b>0</b>
TURN	0	1,550	1,550	3,100	<b>0</b>
UCAN	0	1,550	0	1,550	<b>(1,550)</b>

7  
8 **1. UCAN**

9 Only UCAN takes issue with the VDI Expansion project and recommends that be denied in its  
10 entirety. UCAN bases this recommendation on its misunderstanding of the purpose for the VDI  
11 Expansion project and how it differs from the Digital Workspace project (WP# 00908B).<sup>82</sup> The short  
12 answer is that the two projects are different and the VDI project should not be rejected by the  
13 Commission.

14 SDG&E provided the business justification for both the Digital Workspace project and Virtual  
15 Desktop Infrastructure project in its testimony and Capital workpapers.<sup>83</sup> They are two distinct  
16 projects. While both projects aim to remove technical obsolescence, improve security, performance,  
17 and reliability, the VDI Expansion project focuses on replacing the Company’s virtual desktop solution  
18 that has reached end-of-life, while the Digital Workspace project is focused on replacing older, slower,  
19 out-of-warranty desktop hardware. Specifically, the VDI Expansion project is designed to address  
20 access for contractors who perform work for SDG&E and have a need to directly communicate with  
21 Company systems. This project will replace a technology platform to provide rapid, secure, and  
22 temporary virtual access to Company systems for SDG&E’s temporary contract resources. If the  
23 contractors access SDG&E systems using their own computers not monitored and authorized by  
24 SDG&E, it would pose a serious security risk to the Company’s network and systems, thereby

<sup>82</sup> Ex. UCAN (Woychik) at 304:15-20.

<sup>83</sup> Ex. SDG&E-25-CWP-R (Information Technology), WP # 908B – Digital Workspace, WP # 908C – RAMP - VDI Expansion – Phase 2.

1 jeopardizing Company policies, while increasing compliance risks and the safety of system/data  
2 integrity. In contrast, the Digital Workspace project focuses on replacing EOL devices with new  
3 technologies that can provide faster, secure, supportable, and portable hardware devices to our full-time  
4 employees, allowing the Company's operations to continue efficiently and securely from anywhere, at  
5 any time. SDG&E addressed UCAN's proposal for the Digital Workspace project in Section V (Sub-  
6 section H) above.

7 The VDI Expansion also addresses security and obsolescence concerns due to its modern  
8 architecture, which allows rapid scalability, increased compatibility and automatic update capabilities  
9 and enhance the adaptability and longevity of this technology.

10 UCAN does not object to the 2023 forecast for this project, taking issue only with the 2024  
11 Capital forecast, and if its recommendation were adopted, SDG&E will not be able to implement a  
12 partial VDI system to secure temporary contractors from accessing SDG&E internal network and  
13 systems. SDG&E will continue to have contractors leveraging their own unsecured computers  
14 introducing network vulnerabilities and cybersecurity risk for SDG&E. For the reasons stated above,  
15 SDG&E requests the Commission reject UCAN's position and adopt SDG&E's forecast as reasonable.

16 **J. Select Projects UCAN Challenged for Technology Obsolescence**

17 **1. UCAN**

18 UCAN did not provide any support for its recommendation based on the individual merits or  
19 details of any particular IT capital project proposed by SDG&E.

20 SDG&E's 2022-2024 IT capital request is well-supported by project-by-project information.  
21 SDG&E has provided just under 830 pages of detailed capital workpapers, representing 114 projects.<sup>84</sup>  
22 SDG&E's capital workpapers specifically identify the purpose, description, justification, and types of  
23 investments needed for the forecast period, which UCAN fails to recognize and yet makes broad  
24 assertions without any specific evidence or science provided to support UCAN's statements.<sup>85</sup> SDG&E  
25 also forecasted in-service dates for each project listed in the SDG&E IT 2022-2024 capital forecasts.  
26 SDG&E's direct testimony includes narratives in support of the SDG&E IT-sponsored capital projects.  
27 UCAN's general assertion that the technology SDG&E has selected may become obsolete or stranded  
28 during the course of the GRC is unfounded and insufficient to support UCAN's recommendations.

---

<sup>84</sup> Ex. SDG&E-25-CWP-R (Information Technology).

<sup>85</sup> Ex. UCAN (Zeller) at 14-18.

SDG&E's Capital project forecasts are reasonable and well-supported by the record and should be adopted by the Commission.

This section of rebuttal testimony supports SDG&E's IT Capital costs listed in Table BG-WE-16. The business justification for these projects is sponsored in the direct and rebuttal testimony and work papers listed in Table BG-WE-15.

Only UCAN challenges the Capital projects listed in Table BG-WE-15 below. UCAN states it generally opposes SDG&E's IT Capital forecast for these select by making broad statements about technology obsolescence, stranded assets, and its recommendation to disallow authorization for Capital investments. These assertions are contained in various places throughout UCAN's testimony without any specific evidence or science provided to support UCAN's statements. The Commission should disregard UCAN's unsupported attempt to challenge the projects contained in Table BG-WE-15, based on its concern that technology becomes obsolete.

**Table BG-WE – 15  
Select projects challenged for Technology Obsolescence**

<b>Capital Work Paper (WP) #</b>	<b>Project Name</b>	<b>Testimony Name</b>	<b>Direct Testimony Exhibit #<sup>86</sup></b>	<b>Rebuttal Testimony Exhibit #</b>
920AF	California Independent System Operator (CAISO) Mandates 2024	Energy Procurement	SDG&E-10	SDG&E-210
920A	Microgrid Portal	Electric Distribution Capital	SDG&E-11-R	SDG&E-211
920AJ & 920X	Distribution Interconnection Info. System (DIIS) - Rule 21 and NEM Enhancements	Electric Distribution O&M	SDG&E-12-R	SDG&E-212
920B & 920C	Smart Grid Operations (Product Team)	Electric Distribution O&M	SDG&E-12-R	SDG&E-212
908T	Electric Grid Ops Small Cap 2024	Electric Distribution O&M	SDG&E-12-R	SDG&E-212
920BA	Distributed Energy Resource Management System (DERMS)	Electric Distribution O&M	SDG&E-12-R	SDG&E-212
920R	Vegetation Management - Work Management (Product Team)	Wildfire Mitigation and Vegetation Management	SDG&E-13-2R	SDG&E-213

<sup>86</sup> The business justification for these projects is sponsored in the direct and rebuttal testimonies as listed in Table BG-WE – 15.



Capital Work Paper (WP) #	Project Name	Testimony Name	Direct Testimony Exhibit # <sup>86</sup>	Rebuttal Testimony Exhibit #
920AU, 920L, 920Y	Local Area Distribution Controller (LADC)	Clean Energy Innovations	SDG&E-15-R	SDG&E-215
903H	Clean Transportation Product Team 2023-2024 (Product Team)	Clean Transportation	SDG&E-21	SDG&E-221
907A	IT Quality & Continuous Testing Platforms	Information Technology	SDG&E-25	SDG&E-225
907M	Cloud Data Lake	Information Technology	SDG&E-25	SDG&E-225
908X	Cloud Foundations	Information Technology	SDG&E-25	SDG&E-225
920P	Digital Asset and Damages Detection Platform	Information Technology	SDG&E-25	SDG&E-225
908W	Infrastructure as a Service Implementation (IaaS)	Information Technology	SDG&E-25	SDG&E-225
920F	Construction, Planning and Design (CPD) Enhancements (Product Team)	Safety, Risk & Asset Management Systems	SDG&E-31-R	SDG&E-231
920H	Field Mobile Hardware Replacement	Safety, Risk & Asset Management Systems	SDG&E-31-R	SDG&E-231
920M	GIS Modernization (Product Team)	Safety, Risk & Asset Management Systems	SDG&E-31-R	SDG&E-231
920E	Investment Prioritization	Safety, Risk & Asset Management Systems	SDG&E-31-R	SDG&E-231

**Table BG-WE – 16**  
**Capital forecast for projects listed in Table BG-WE – 15 (Ex. SDG&E-25)**  
**Constant 2021 (\$000)**

Capital Work Paper (CWP) #	Project Name	2022	2023	2024
920AF	California Independent System Operator (CAISO) Mandates 2024	0	0	1,456
920A	Microgrid Portal	593	389	0

1  
2  
3  
4

<b>Capital Work Paper (CWP) #</b>	<b>Project Name</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>
920AJ & 920X	Distribution Interconnection Info. System (DIIS) - Rule 21 and NEM Enhancements	1,325	1,570	1,409
920B & 920C	Smart Grid Operations (Product Team)	2,619	2,619	2,369
908T	Electric Grid Ops Small Cap 2024	0	0	440
920BA	Distributed Energy Resource Management System (DERMS)	3,064	2,810	3,138
920R	Vegetation Management - Work Management (Product Team)	0	5,754	1,678
920AU, 920L, 920Y	Local Area Distribution Controller (LADC)	1,068	2,040	897
903H	Clean Transportation Product Team 2023-2024 (Product Team)	0	1,186	1,612
907A	IT Quality & Continuous Testing Platforms	1,967	779	995
907M	Cloud Data Lake	0	2,500	2,500
908X	Cloud Foundations	5,968	4,812	5,312
920P	Digital Asset and Damages Detection Platform	4,505	3,680	3,680
908W	Infrastructure as a Service Implementation (IaaS)	0	0	2,000
920F	Construction, Planning and Design (CPD) Enhancements (Product Team)	0	1,643	1,971
920H	Field Mobile Hardware Replacement	0	3,489	3,544
920M	GIS Modernization (Product Team)	1,563	2,344	324
920E	Investment Prioritization	1,873	5,502	9,256

1  
2 SDG&E requests the Commission to reject UCAN's position for the select projects listed in  
3 Table BG-WE-15 above and adopt SDG&E's forecast as reasonable. No other party objected to the  
4 Capital project forecasts listed above in Table BG-WE-16.

1 **VI. CONCLUSION**

2 SDG&E has addressed the proposed recommendations presented by parties and demonstrated  
3 that their proposals are not warranted. The Commission should disregard the parties recommendations  
4 and determine that SDG&E’s forecast for Capital and O&M expenditures is reasonable and should be  
5 adopted in its entirety. The Commission should also recognize that any disallowance recommended by  
6 the parties for SDG&E to invest in operations and technology may lead to increased risks,  
7 cybersecurity threats, and inefficiencies in our systems, and may also have a direct impact in the  
8 delivery of reliable, safe, efficient, and secure services to our customers.

9 SDG&E has met the burden of proof by providing adequate justification and support for  
10 SDG&E’s IT costs in my direct testimony and work papers (Ex. SDG&E-25, SDG&E-25-WP, and  
11 SDG&E-25-CWP-R). Furthermore, the Company has presented clear and convincing evidence through  
12 this rebuttal and various intervenor data request responses that SDG&E’s Capital forecast expenditures  
13 are just and reasonable.

14 In conclusion, SDG&E has demonstrated the following:

- 15 • SDG&E’s TY 2024 Shared Services O&M forecast of \$83.305 million is  
16 reasonable.
- 17 • SDG&E’s TY 2024 Non-Shared Services O&M forecast of \$27.113 million is  
18 reasonable.
- 19 • SDG&E’s 2022 Capital forecast of \$220.012 million is reasonable.
- 20 • SDG&E’s 2023 Capital forecast of \$208.793 million is reasonable.
- 21 • SDG&E’s 2024 Capital forecast of \$214.186 million is reasonable.

22 This concludes my prepared rebuttal testimony.

**APPENDIX A**  
**GLOSSARY OF TERMS**

ACRONYM	DEFINITION
A	Application
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
CA	Cal Advocates
CAISO	California Independent System Operator
CAPP	California Arrearage Payment Program
CCA	Community Choice Aggregation
CCC	Customer Contact Center
CCotF	Contact Center of the Future
CEN	Customer Energy Network
CFF	Cross Functional Factor
C&I	Commercial and Industrial
CIO	Chief Information Officer
CIS	Customer Information System
CISBA	Customer Information System Balancing Account
COKE	Centralized Operations KPIs & Exception
Commission	California Public Utilities Commission
CPD	Construction, Planning and Design
CPUC	California Public Utilities Commission
CSFO	Customer Services Field Operations
CSOO	Customer Services Office Operations
CWP	Capital Work Paper
D.	Decision
DERMS	Distributed Energy Resource Management System
DIIS	Distribution Interconnection Info. System
DR	Data Request
EOL	End-of-Life
EOS	End-of-Support
FSD	Field Service Delivery
FTS	Foundation Technology System
GIS	Geographic Information System
GRC	General Rate Case
IaaS	Infrastructure as a Service
IT	Information Technology
IVR	Interactive Voice Response
KPI	Key Performance Indicator
LADC	Local Area Distribution Controller
MCAM	Modified Cost Allocation Mechanism
MDMS	Meter Data Management System
NEM	Net Energy Metering

<b>ACRONYM</b>	<b>DEFINITION</b>
OIR	Order Information Record
OWCE	OpenWay Collection Engine
PAO	Public Advocates Office
RAMP	Risk Assessment Mitigation Phase
RFP	Request for Proposal
SAP	Systems, Applications, and Products
SDG&E	San Diego Gas & Electric Company
SM 2.0	Smart Meter 2.0
SoCalGas	Southern California Gas Company
SOX	Sarbanes-Oxley
TLS	Transport Layer Security
TOU	Time of Use
TURN	The Utility Reform Network
TY	Test Year
UCAN	Utility Consumer's Action Network
VDI	Virtual Desktop Infrastructure
WECO	Wathour Engineering Co.
WP	Work Paper

**APPENDIX B**  
**GLOSSARY OF DEFINITIONS**

<b>TERM</b>	<b>DEFINITION</b>
Agile	A group of software development methodologies based on iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.
Cloud	Refers to software and services that run on the Internet, instead of locally on a computer. Most Cloud services can be accessed through a Web browser like Firefox or Google Chrome, and some companies offer dedicated mobile apps.
Epic	A body of work that can be broken down into specific tasks (called user stories) based on the needs/requests of customers or end-users.
Feature	A feature is a service or function of the product that delivers business value and fulfils the customer's need.
Infrastructure as a Service (IaaS)	A model in which a third-party provider hosts servers, storage, and other virtualized compute resources and makes them available to customers over the internet.
Product Team	A product team is an ongoing, dedicated team responsible for both enhancements and support of a product.
Technical Debt	Technical Debt ( <i>i.e.</i> , Tech Debt) is defined as any Company hosted hardware or software that has reached manufacturer End of Life (EOL) or End of Support (EOS); therefore, the vendor no longer provides support or security updates. Tech Debt presents a serious risk to our Company because it increases operational costs as well as cyber risks & vulnerabilities.
Two-Factor Authentication	An identity and access management security method that requires two forms of identification to access resources and data.

**APPENDIX C**  
**INDUSTRY EXPERT RESEARCH & REFERENCES**

- Appendix C-1 – Gartner - Securing End of Support Production Systems
- Appendix C-2 – Department of Homeland Security - CISA – Bad Practices.pdf
- Appendix C-3 – Gartner – Research Roundup Top 10 Trends Shaping the Utility Section in 2023.pdf

# Securing End-of-Support Production Systems

Published 15 March 2023 - ID G00782821 - 15 min read

By Analyst(s): Evgeny Mirolyubov, Neil MacDonald, Tony Harvey

Initiatives: [Infrastructure Security](#)

Security risks increase as production systems reach the end of their manufacturer support life cycle quicker than the business can replace or retire them. Security and risk management leaders must collaborate with the infrastructure team to minimize the attack surface of end-of-support systems.

## Overview

### Key Findings

- Security and risk management leaders are frequently unaware of the business-critical systems running on unsupported operating systems and applications, causing technical debt in the organization.
- Interdependencies between operating systems, applications and middleware components often make upgrading just one end-of-support (EoS) component unworkable, requiring an upgrade of the entire system.
- Migrating business-critical applications from an EoS system may be impractical, requiring business leaders to continue to operate EoS systems while migration plans and funding are finalized.
- EoS systems are significantly more susceptible to compromise, becoming the gateway for broader operational and business disruptions.

### Recommendations

Security and risk management leaders responsible for infrastructure security should:

- Collaborate with the infrastructure and enterprise architecture teams to maintain an updated inventory of production systems and EoS dates. Integrate IT asset management (ITAM) and unified endpoint management (UEM) data sources to create a holistic asset view.



- Decide which EoS systems to retire and which must continue to operate by working with business counterparts to define a risk profile for each system. At the minimum, assess business criticality, the volume and frequency of use, and connectivity requirements.
- Reduce the attack surface of each EoS system remaining in production, including those scheduled for retirement, by applying compensating security controls.
- Prepare and practice incident response and recovery procedures to identify tooling and procedure changes required for EoS production systems.

## Strategic Planning Assumption

By October 2026, 75% of organizations using Microsoft Windows Server 2012 R2 will have yet to complete migrations to a supported platform.

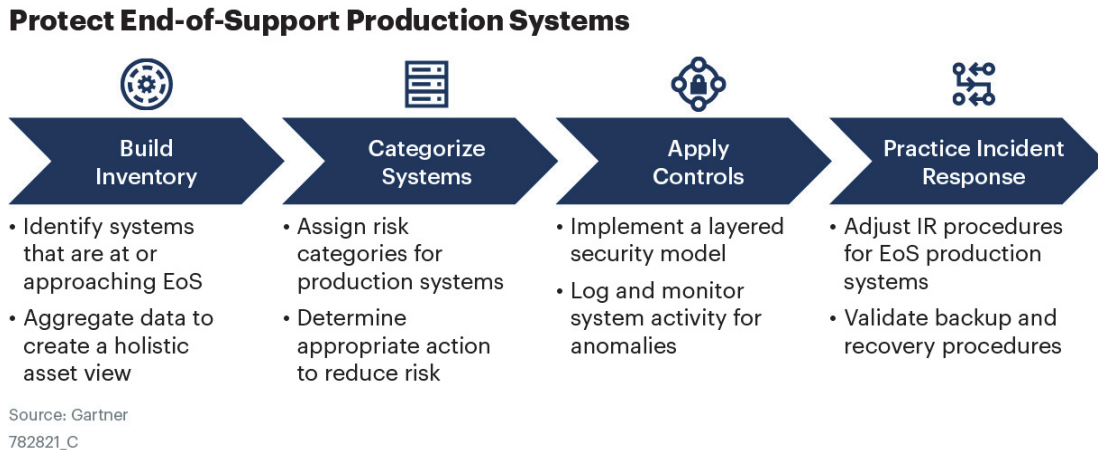
## Introduction

All technology becomes obsolete and unsupported over time. While every security and risk management leader recognizes the truth in this statement, Gartner clients often mention that they are running end-of-support (EoS) production systems. <sup>1</sup> Unsupported systems do not receive bug fixes, enhancements, and, most importantly, security patches – significantly increasing the risk of system compromise. <sup>2,3</sup>

While migration to a supported platform is recommended, it's usually difficult to justify the costs against the inherent risk. Upgrades are complex and sometimes not possible due to how applications were architected and the relationship between the app, operating system (OS) and middleware. Even if the application vendors support the updated OS, for business-critical systems this is a major operation that will require extensive testing. If the application vendor does not support the updated OS, then the application must be upgraded, which could require the database to be upgraded. What started as a simple OS upgrade has now become a complex multiyear program to upgrade the core ERP systems. Business applications seldom operate in isolation, and interdependencies between other applications and tools in enterprise environments will often make upgrading a very daunting task.

To protect EoS systems, security and risk management leaders must work with IT and business counterparts to maintain an updated asset inventory, categorize systems according to the level of risk, and apply compensating security controls (see Figure 1). Once implemented, each security layer needs to be continuously monitored and tested, and the security policies should be adjusted as new threats appear.

Figure 1. Protect End-of-Support Production Systems



## Analysis

### Inventory Production Systems

Security and risk management leaders need to inventory and assess their entire technology estate to identify components and systems that are either at or approaching EoS. This can be done using a variety of tools including: IT asset management (ITAM), software asset management (SAM), unified endpoint management (UEM), and threat and vulnerability management (TVM). Data should be aggregated into a configuration management database (CMDB) or enterprise architecture tool to create a holistic view that includes dependencies (see [ITSM Best Practices: A Guidance Framework for Implementing a Configuration Management Database](#)).

Examine the four layers for each production system:

- Hardware** – Is the hardware still under warranty or being supported by the vendor or reputable third party, are spares available and are firmware updates still being delivered?
- Operating system** – This is the most common attack vector, which makes availability of security patches and configuration baselines a critical requirement.
- Middleware** – Databases, web services, and other middleware can become unsupported but still need patching and vendor or third-party support. SolarWinds and Log4j offer observability technology that exemplifies how unmanaged middleware can introduce significant risk.

- **Application** — Is the application still supported by the vendor, or is the source code still available to implement security fixes if it is a custom in-house application?

Most vendors publish EoS announcements with ample time to prepare for migration, and include recommendations on the migration path when available. Record the EoS date, system dependencies, and other relevant information for every system in the environment. Then, create reminders to ensure systems are upgraded, migrated or retired before EoS. Gartner also recommends that all EoS systems that remain in use are documented on a risk register to maximize transparency.

## Categorize Systems According to the Level of Risk

Once the system inventory is built, organizations need to place each supported and unsupported system into one of the following risk categories:

- **High risk** — Systems that are internet-facing and/or contain trade secrets, intellectual property, personally identifiable or other regulatory data, are highly trusted by other systems, or are critical to running the business.
- **Medium risk** — Systems that contain public data and/or provide internal services to employees and systems that are trusted by other internal systems but not externally exposed.
- **Low risk** — Systems with limited users and functionality that provide noncritical services or are easily recoverable or replaceable.

As systems start to approach the end of their manufacturer support life cycle, determine the appropriate response action. Any EoS system that can be virtualized should be. While virtualization does not intrinsically make a system more secure, it provides several advantages. Virtualized systems remove dependencies on hardware, which may be out of support, and offer ways for system managers to take system snapshots that can be quickly restored in the event of a breach.

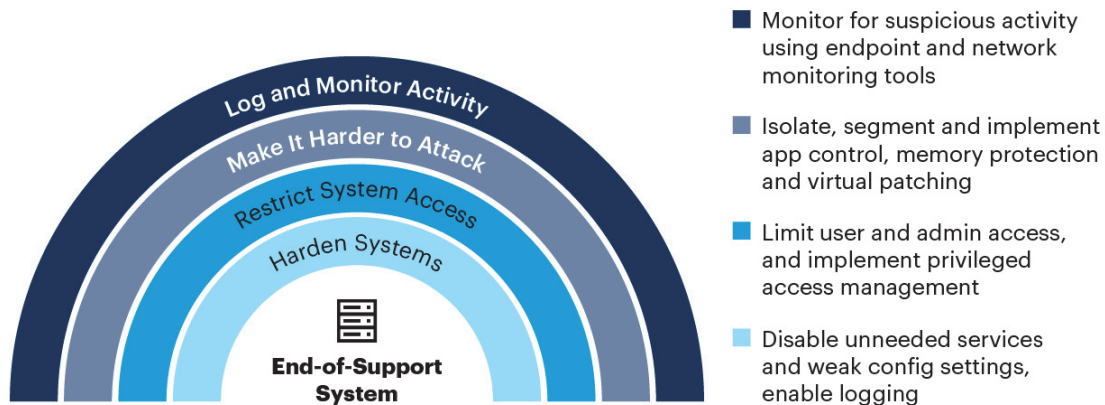
Organizations must also identify production systems that are not delivering useful work for the business, commonly referred to as “zombie servers/virtual machines (VMs).” Identifying and decommissioning these systems should be a priority, as removing them removes the associated security risk and can result in significant operational savings.

## Apply Compensating Controls to Reduce Risk

Each system that cannot be retired or virtualized should have a layered security approach applied (see Figure 2), starting with the highest-risk systems. While it may seem that protecting low-risk systems is an unnecessary expense, any vulnerable system represents an extensive attack surface for threat actors wishing to gain an easy foothold into an organization to attack other systems, deploy ransomware, etc.

**Figure 2. Adopt a Layered Security Approach**

### Adopt a Layered Security Approach



Source: Gartner  
782821\_C

**Gartner.**

Security and risk management leaders must consider the following factors when prioritizing compensating controls for each system:

- Ownership of the system (self versus third party)
- Each system's level of risk (high, medium, low)
- Remaining support time for systems approaching EoS
- The impact of selected compensating controls on the system
- Protection levels with compensating controls that are already applied to each system
- Compatibility of compensating controls with the EoS system

The life cycle and supportability of compensating security controls used for protection of legacy production systems is equally important. Organizations looking to continue using compensating controls already available to them should discuss the following points with prospective suppliers prior to making new purchases or commitments:

- Does the vendor have a roadmap for the solution selected as the compensating control? Or has the solution already reached end-of-life with no further enhancements planned for it by the vendor?
- Does the vendor continue to issue maintenance releases, logic updates and security patches to address discovered vulnerabilities; especially privilege escalation for agent-based controls?
- Does the vendor provide technical support in case of compatibility or deployment issues?
- Does the system require administrative rights or internet connectivity? Is a proxy or a gateway available for those that don't have the required connectivity?
- Does the solution rely on management consoles, database servers or any other vendor infrastructure that is itself planned for discontinuation?

The list above is not exhaustive and will change as new attack methods emerge. For the latest guidance, Gartner clients should schedule analyst inquiries to learn about the latest threats and how to combat them.

The compensating controls for EoS production systems fall into the areas described in the sub-sections below:

- Harden systems
- Restrict system access
- Make it harder to attack
- Log and monitor activity

## **Harden Systems**

Misconfigurations are a frequent cause of system vulnerabilities. To reduce the attack surface, harden system configurations by disabling unnecessary services and removing default configurations. For example, if system services and unused software and drivers are uninstalled or disabled, then even if there is an exploit that targets those services, your systems are not vulnerable. Make your EoS systems more resilient to attacks and eliminate the root cause of many vulnerabilities by defining and implementing security hardening policies for all end-user endpoints and servers.

Use unified endpoint management (UEM) tools to deploy hardening scripts, Administrative Template XML-Based (ADMX) policies or prehardened OS images. Utilize off-the-shelf hardening standards, such as Microsoft Security Baselines,<sup>4</sup> Center for Internet Security (CIS) Benchmarks,<sup>5</sup> or DISA Security Technical Implementation Guidelines (STIGs) to uninstall and/or disable unneeded device drivers, services, software, and capabilities.<sup>6</sup>

Continue to patch any supported software that still remains on the EoS system. For example, if the OS is out of support, applications running on the OS may still be supported and should be patched.

### **Restrict System Access**

Restrict system access to authenticated users, and to only those users and groups that require explicit access. Use a privileged access management (PAM) system or significantly reduce administrative access and permissions, including system-level support accounts and service accounts. Ensure that any administrator accounts and passwords are unique to each system to prevent credential reuse in the event of a breach. Restrict physical access to the systems as well. For more information on privileged access management see [Guidance for Privileged Access Management](#).

For administrative access, mandate the use of a “jump” server running an up-to-date supported OS to manage EoS systems to further increase security. Remove the ability of administrators to connect to management interfaces of EoS systems via any other route. This makes network communication patterns predictable and, thus, easy to monitor.

### **Make It Harder to Attack**

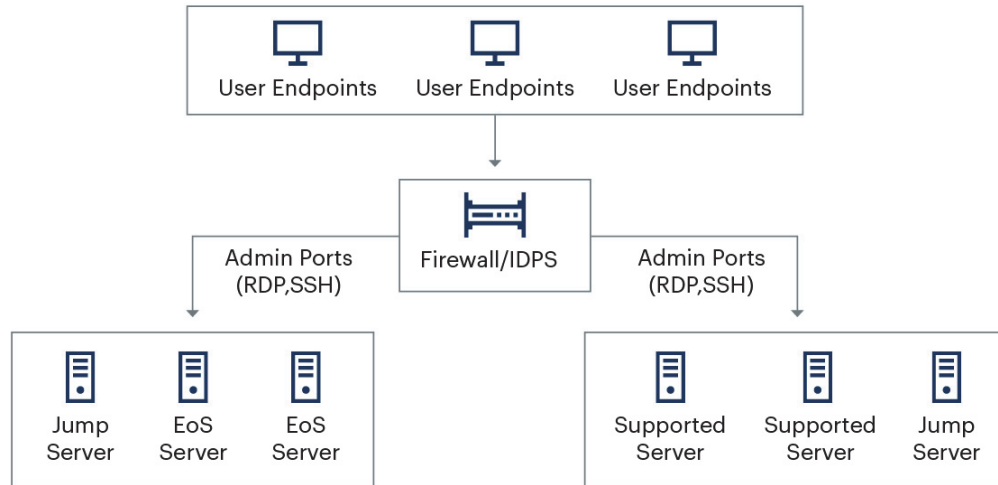
Use a cloud-native application protection platform (CNAPP) to provide consistent visibility and control of all production server workloads, both in the data center and the cloud, and protect against attacks. Assess and deploy CNAPP attack surface reduction functions, including the following:

- **System integrity assurance** – Ensures that the underlying hardware, firmware, hypervisor and VM have not been modified prior to boot up, and monitors critical system and configuration files while the system is running.
- **Application control/allow-listing** – Prevents threat actors from executing applications not on the allow list. Legacy production systems typically have a predictable set of trusted processes making these systems a good fit for allow-listing.
- **Exploit prevention/memory protection** – Prevents attacks attempting to exploit trusted applications running in the system’s memory space, and reduces risks of fileless and memory injection attacks and obfuscated malware.
- **Host-based intrusion protection system with vulnerability shielding** – Provides deep network traffic inspection to each VM and implements “virtual patching” capability to protect systems against attacks on known vulnerabilities.

To reduce lateral movement and network exposure, protect EoS systems using network segmentation. Segmentation is the creation of zones in a network that contains workloads or other assets that need to be isolated from the rest of the environment. Isolate EoS systems behind a firewall and restrict network access to these known vulnerable segments (see Figure 3). The basic principle for a segment containing EoS systems is to be in a default deny mode where all ports, protocols, IP addresses and MAC addresses are denied access unless specifically required for the system to operate.

Figure 3. Network Segmentation Example

### Network Segmentation Example



Source: Gartner  
782821\_C

Gartner.

For high-security environments, apply network microsegmentation to segregate higher-risk systems from other systems in the same network segment. By using microsegmentation, if an attacker breaches the enterprise network, you can reduce the level of impact by making it harder for the attacker to spread laterally.

Network firewalling and microsegmentation are also a core element of the server workload protection strategy and are often included as a part of microsegmentation solutions (see [Emerging Tech: Adoption Growth Insights for Microsegmentation](#) for more information).

To protect legacy end-user endpoints, select and deploy an appropriate endpoint protection technology. Such solutions provide a level of prevention and detection, help meet internal and external audits, and serve for an acceptable period of use until the EoS endpoints are upgraded. Ensure that the endpoint protection vendor continues to issue security patches, detection content updates, and bug fixes during the remaining lifetime of the legacy endpoints retained (see [Magic Quadrant for Endpoint Protection Platforms](#) for more information).

### Log and Monitor Activity



Prioritize legacy environments when assessing your monitoring strategy. Even the most basic host-level monitoring can make a big difference when dealing with active threats in the environment.

Behavioral monitoring is an advanced capability of modern CNAPP (runtime workload protection functionality) and endpoint protection platform (EPP) tools (detection and response functionality) that identify deviations from normal behavior by continuously analyzing network communications, processes launched, files opened and other behavioral patterns that indicate early signs of malicious activity. Security and risk management leaders should require CNAPP and EPP vendors to provide transparency on the differences in behaviors monitored and threat intelligence available for unsupported systems in comparison to a modern OS agent. Then, be prepared to supplement vendor threat intelligence with custom detection rules if the product functionality permits that.

Consider alternative monitoring technologies, such as network detection and response (NDR), especially for legacy systems that don't allow an agent installation. Even if the infrastructure is not adequately segmented, visibility into network traffic patterns and host-level activities will provide security leaders with an early warning system for abnormal behaviors. By implementing the compensating controls mentioned in this note, organizations should expect fewer deviations from normal behavior and a relatively predictable environment, which means the detections are more likely to be true positives.

## Prepare and Practice Incident Response Procedures

Expect to be breached and be ready to perform a root cause analysis to identify and address the source of the exploited vulnerability (technology, process or people) and what methods might be used to prevent a recurrence. Security and risk management leaders must assess and document the impact of dealing with unsupported systems on incident response procedures and tools. For example, alert data collected from EoS systems may be less detailed due to limitations in security tool capabilities, impacting detection engineering and alert escalation processes. Incident declaration thresholds may differ, given the heightened risks associated with legacy systems. Containment, analysis and response workflows are likely to require additional expertise about the systems under attack and the methods of implementing these procedures.

Resource-constrained security teams should evaluate a managed detection and response (MDR) service to complement internal monitoring efforts with 24/7 coverage and expertise (for additional guidance, see [Market Guide for Managed Detection and Response Services](#)). Additionally, procure incident response retainer services in advance to supplement your team with external expertise when you need it most.

See [How to Create an Incident Response Plan](#) for more information on incident response planning and operations.

As a part of the strategy to protect EoS systems, the ability to restore compromised systems to a known good state is also required. Continue to back up EoS systems using existing tools. However, backing up physical installations relies on agents installed in the host operating system, which may not be supported in modern backup applications. For example, support for backing up endpoints like Windows XP is rapidly disappearing. So be prepared to keep a small footprint of the existing backup system available if you plan to replace it with a more modern alternative. Using disk imaging software for backup purposes, especially in the case of proprietary OT devices, like medical scanners and other OT device types, presents a viable alternative. Organizations must also update their backup and recovery procedures to account for these limitations in available backup approaches for EoS systems.

In the event of a system breach that bypasses all the compensating controls above, be prepared to migrate to a newer, supported version of the system. Proactively testing and training for such a scenario will help minimize downtime and impact on the business.

For backup strategy planning, see [Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware](#).

## Evidence

<sup>1</sup> Many production systems are running on near-end-of-support OS, such as Windows Server 2012/R2, which will be end of support on 10 October 2023. Unless migration projects are nearly complete, these systems will continue to be used in production after the end-of-support date. Most vendors will sell extended support at a high cost for a limited time (in the case of Windows 2012/R2, that is October 2026).

[SQL Server 2012 and Windows Server 2012/2012 R2 End of Support](#), Microsoft.

[Windows Server 2012 R2](#), Microsoft Product Life Cycle.

<sup>2</sup> “In 2021, for example, over 17% of newly discovered vulnerabilities were over five years old.”

“ninety-seven percent of successful credential stuffing attacks involve legacy authentication.”

[How Secure Are Your Legacy Systems?](#), Morphisec Breach Prevention Blog.

<sup>3</sup> “Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.”

[Bad Practices](#), CISA

<sup>4</sup> [Using Security Baselines in Your Organization](#), Microsoft.

<sup>5</sup> [CIS Benchmarks List](#), Center for Internet Security.

<sup>6</sup> [Security Technical Implementation Guides \(STIGs\)](#), The DoD Cyber Exchange.

## Document Revision History

[Securing End-of-Support Production Systems - 24 December 2019](#)

---

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

[A Guidance Framework for Developing and Implementing Vulnerability Management](#)

[Prepare for Windows Server 2012 End Of Support](#)

[Magic Quadrant for Endpoint Protection Platforms](#)

[Emerging Tech: Adoption Growth Insights for Microsegmentation](#)

[How to Successfully Deploy Application Control](#)

---

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."



## Bad Practices

Recent attacks on the water we drink, our food production, our healthcare availability, our schools, our municipalities, and other national critical functions have demonstrated cyberattacks against critical infrastructure can have a significant impact on the critical functions of government and the private sector. All organizations, and particularly those supporting designated Critical Infrastructure or National Critical Functions (NCF)<sup>[1]</sup>

[https://www.cisa.gov/badpractices#\\_ftn1](https://www.cisa.gov/badpractices#_ftn1) should implement an effective cybersecurity program to protect against cyber threats and manage cyber risk commensurate with the urgency of those NCFs to national security, national economic security, and/or national public health and safety.

CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting Critical Infrastructure or NCFs. The presence of these Bad Practices in organizations that support Critical Infrastructure or NCFs is exceptionally dangerous and increases risk to our critical infrastructure. We rely on these critical infrastructures for national security, economic stability, and life, health, and safety of the public. Entries in the catalog will be listed here as they are added.

1. Use of unsupported (or end-of-life) software in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
2. Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and National Critical Functions is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.
3. The use of single-factor authentication for remote or administrative access to systems supporting the operation of Critical Infrastructure and National Critical Functions (NCF) is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet.

While these practices are dangerous for Critical Infrastructure and NCFs, CISA encourages all organizations to engage in the necessary actions and critical conversations to address Bad Practices.\*

\*This list is focused and does not include every possible inadvisable cybersecurity practice. The lack of inclusion of any particular cybersecurity practice does not indicate that CISA endorses such a practice or deems such a practice to present acceptable levels of risk.

On our CISAgov GitHub <<https://github.com/cisagov/bad-practices/discussions>>, we opened a Bad Practices discussion page to engage with administrators and IT professionals from industry, federal government and state, local, tribal and territorial governments. Our intent is to gather your perspectives and input on this initiative as well as discuss how to eradicate these practices.

---

[1] <[https://www.cisa.gov/badpractices#\\_ftnref1](https://www.cisa.gov/badpractices#_ftnref1)> National Critical Functions | CISA  
<<https://www.cisa.gov/national-critical-functions>>

## CONTACT </stopransomware/contact-us>



About CISA </about>

DHS.gov  
<<https://www.dhs.gov>>

Accessibility  
<<https://www.dhs.gov/accessibility>>

FOIA Requests  
<<https://www.dhs.gov/foia>>

Budget and Performance  
<<https://www.dhs.gov/performance-financial-reports>>

No FEAR Act </cisa-no-fear-act-reporting>

Office of Inspector General  
<<https://www.oig.dhs.gov/>>

Privacy Policy </privacy-policy>

Subscribe

The White House  
<<https://www.whitehouse.gov/>>

USA.gov  
<<https://www.usa.gov/>>

Website Feedback  
</forms/feedback>



# Research Roundup: Top 10 Trends Shaping the Utility Sector in 2023

Published 25 January 2023 - ID G00784272 - 11 min read

By Analyst(s): Nicole Foust, Zarko Sumic

Initiatives: [Energy and Utilities Digital Transformation and Innovation](#)

Utilities are faced with unprecedented challenges and opportunities shaped by continued disruption. Utility CIOs should use this research to prioritize and align IT to the needs of the business, including architecture, roadmaps and resources, as they build a sustainable utility future.

## Analysis

In 2023, power and water utilities will continue to face a variety of forces that will challenge their business and operating models and shape their technology investments. Disruptions such as the COVID-19 pandemic, economic recession, and the Russian invasion of Ukraine, as well as consequent energy crises cast a backdrop on an already challenging business and operating environment for utilities.

For energy utilities, challenges are primarily consequences of energy transition driven by 4D forces (decarbonization, decentralization, digitalization and democratization; see Note 1). For water utilities, challenges stem primarily from access to water and security management. Further, all utilities globally are facing increasing business costs, an aging and exiting workforce, expensive and hard-to-find talent, economic disruption and volatility, increasing physical and cyber-physical risk, and an unstable regulatory regime, contributing to a challenging environment.

Operationally, the pressure is mounting to maintain physical integrity and modernize aging grid infrastructure in the face of shifting consumption/production patterns, the accelerated deployment of renewable energy assets at utility scale, and at the grid edge. Water operations are being pressed to redress old issues like stemming leakage while addressing renewed concerns and capabilities to handle effluents and contamination. Natural gas faces the triple priority of infrastructure renewal, security management and network revision for the emerging hydrogen economy.

These challenges can be grouped into three key themes: lack of resilience to changes in physical and business environment, out-of-date technologies, and emerging customer needs that are underserved. For these reasons, creating new value propositions and improving engagement for a customer base that is awakening to more information, capability and agency continues to be one of the top goals for utility executives.

These pressures, coupled with regulatory uncertainty and political interference, are reshaping business and operating models, and requiring utilities to develop new ways of thinking, new skills and capabilities. As a result, utility organizations are redoubling their focus on delivering mission-critical, technology-furnished capabilities to supply commodities to their customer base, while enabling them to reposition for a sustainable future provisioning of energy and water.

---

*Intelligent operations is a strategic goal for utility CIOs that must shape digital investments toward fit-for-the-future cyber-physical asset designs.*

---

Utilities continue investing in digital technologies, according to the 2023 Gartner CIO and Technology Executive Survey. <sup>1</sup> The purpose of the investments is to ensure the ability to provide available, affordable and acceptable services to the customers they serve by increasing agility, performance and opportunities during the unpredictable and volatile energy and water transition period.

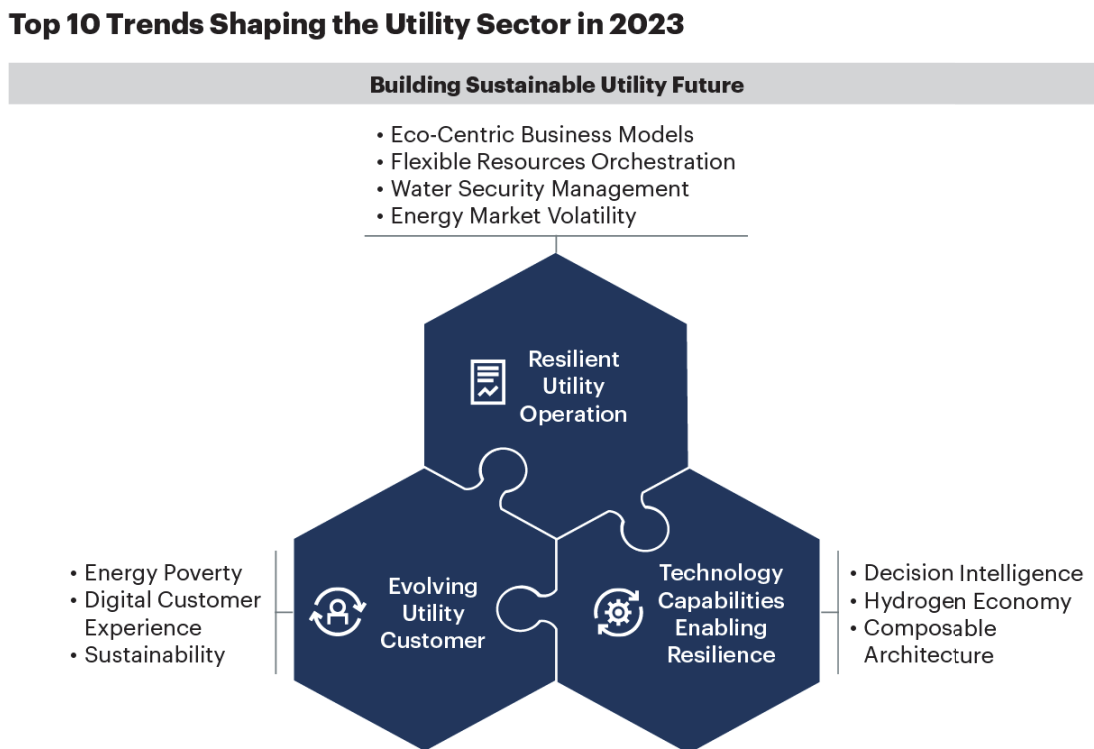
A sustainable utility future requires improved business resilience and the ability to quickly change to address new requirements arising from the energy transition and from increasing regulatory and political demands. Utilities must shape-shift to increase resilience while maintaining productivity and efficiency.

Utility technology leaders must confidently compose the future for their organizations in the midst of uncertainty during this energy transition volatile period – the future that requires your organizations to be both agile and resilient. This is where utility trends for 2023 can help. In this utility trend research roundup, we explore ten key trends that are shaping utility companies globally in 2023. These can help you set your priorities, explore technology investment directions and compare your position to others in the industry. We've selected these trends for their promise to facilitate your journey as you build a sustainable utility future.

Though these trends are global, they may have different relevance in different regions. They can translate very easily into specific utility domains (e.g., power generation, transmission and distribution, and water and wastewater). And they can fit to different levels of digital ambition (e.g., industry leader, moderate and tailing). Accordingly, not all trends have the same impact on every organization.

Figure 1 highlights the alignment between industry trends and the challenge they show promise to resolve. Trends that are building sustainable utility futures can be clustered into three strategic business imperatives: resilient utility operation, technology capabilities enabling resilience and evolving utility customers.

**Figure 1: Top 10 Trends Shaping the Utility Sector in 2023**



Source: Gartner  
784272\_C

Utility CIOs and technology leaders must drive a sustainable future by clearly articulating the secure foundation, composable roadmap and momentum toward software-defined assets and intelligent operations that will fulfill business strategies and goals. Utility companies can map these trends to their business requirements by considering three strategic imperatives (see Note 2).

## Research Highlights

*Some recommended content may not be available as part of your current Gartner subscription.*

Each of the trends is explained in more detail in the documents highlighted and linked below. These documents assess the business context for the trend, clarify its description, explain why it is trending now and justify its inclusion among the collection of top trends for utilities in 2023. Each note also clarifies the implications for utility CIOs and digital leaders, and provides recommended action steps. Utility CIOs can use this research to better understand the most relevant trends for their company and focus their technology decisions to keep pace with evolving business priorities.

Links to the research notes that analyze the top 10 trends for utility companies are grouped with their associated strategic business imperative. The order they are presented below does not designate relative importance, as each company will have unique priorities based on their asset portfolio, theater of operations and strategic plans.

### Top 10 Trends Shaping the Utility Sector in 2023

#### Resilient Utility Operation

##### [2023 Utility Trend: Utility Business Models Are Evolving From 'Ego-Centric' to Eco-Centric](#)

Democratization of energy provisioning is forcing utilities to evolve business models from internally focused ego-centric business models to externally focused, collaborative, eco-centric business models. CIOs must ensure that their digital technology strategy and technology investments reflect this shift.

##### [2023 Utility Trend: Orchestrate Flexible Resources to Maintain Power System Operational Integrity](#)

Intermittent renewable energy is displacing large-scale fossil-fueled resources that provided inertia and stabilized the grid. With the diminishing role of fossil fuel resources, utility CIOs must support integration of consumer-owned resources with digital IT and operational technology (OT) services.

##### [2023 Utility Trend: Water Security Management Is the Water Industry's Existential Imperative](#)

Effluent management is the new disruptor for water security management in water utilities and the downfall for legacy water management strategies. Failures in water quality will break water utilities overall. Water utility CIOs should use this trend to evaluate how and why water security management is the key challenge and opportunity for water utility enterprises.

## [2023 Utility Trend: Evolving Markets Challenging Traditional Energy Trading Tools](#)

Turbulent geopolitics and the energy transition are resulting in power outages and spot market price shocks that challenge the utility's existing operational and financial agility. Utility CIOs should consider the impacts of electricity market volatility on their IT strategy, operating model and spending.

### **Technology Capabilities Enabling Resilience**

## [2023 Utility Trend: Establish Decision Intelligence Before Chasing Autonomous Business](#)

Decision intelligence is an essential precursor to execution of automation, irrespective of decision execution technology to support intelligent operations. Utility CIOs can use this research to prioritize and manage business demand for decision automation.

## [2023 Utility Trend: Green Hydrogen Expectations Are High, but So Are Challenges](#)

Hydrogen has great potential to ease the energy transition journey, but multiple challenges remain. This research will help CIOs gain a balanced view of opportunities created by government incentives and investors' interest, as well as challenges faced on the road toward a hydrogen economy.

## [2023 Utility Trend: Composable Architecture Delivers Business Agility](#)

Diverse pressures like operational and business challenges, and disruptions triggered by global events, are forcing utilities to adopt new plans focused on agility and resilience. CIOs can use this trend to evaluate how composable architecture can enable flexibility in delivering business outcomes.

### **Evolving Utility Customer**

## [2023 Utility Trend: Growth of Energy Poverty – Focus on Relief, Revival and Renewable Energy](#)

A majority of the population, currently in the Northern hemisphere, is wrestling with the challenges caused by the lack of access to fuel, food and finance. Energy poverty is the core problem. Utility CIOs can use this research to understand approaches with a dual focus on addressing affordability concerns, as well as ensuring their financial and operational stability.

## 2023 Utility Trend: Digital Customer Experience Is Remodeling for the Energy and Water Transition

For years, customer engagement has been focused on customer service while managing a narrow scope of commodity transactions. But during this era of transition, customer experience (CX) will define the breakout enterprise. CIOs can use this research to design a CX/total experience (TX) that syncs with the energy and water transition.

## 2023 Utility Trend: Sustainability Is a Double-Edged Sword for Utilities

Tightening regulations, stakeholder scrutiny and climate change impacting assets and infrastructure frame environmental challenges, with changing customer attitudes making opportunities for utilities. Utility CIOs should align digital strategies and technology investments with climate change risks.

## Evidence

This research was developed using a combination of evidence including information from analyst interactions with energy and utility companies and technology providers from 1 January through 15 December 2022, as well as analysts' secondary research.

<sup>1</sup> **2023 Gartner CIO and Technology Executive Survey.** This survey was conducted to help CIOs and technology executives overcome digital execution gaps by empowering and enabling an ecosystem of internal and external digital technology producers. It was conducted online from 2 May through 25 June 2022 among Gartner Executive Programs members and other CIOs. Qualified respondents were each the most senior IT leader (e.g., CIO) for their overall organization or some part of their organization (for example, a business unit or region). The total sample was 2,203 respondents, with representation from all geographies and industry sectors (public and private), including 71 from utilities. *Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

## Note 1: The Energy Transition Defined

The energy researcher, Vaclav Smil, has defined the energy transition as the structural change of energy provisioning systems. In this particular case, it refers to the shift from current energy production systems that rely primarily on nonrenewable energy sources (oil, natural gas and coal) to an energy mix based largely on renewable energy sources. The current energy transition is focused on decarbonizing the energy sector at a global level, reducing carbon emissions and ensuring climate stabilization by moving from fossil-based to zero-carbon fuel sources by the second half of this century. The shift will be enabled by a combination of policy frameworks, market instruments, innovation and technology.

## Note 2: Strategic Imperatives to Consider When Mapping Utility Trends to Business Requirements

- **Resilient Utility Operation.** The four trends aligned to this opportunity show promise in resolving key challenges associated with nonresilient business models. The shift is from the traditional utility mantra of “built to last” toward one that is “built for change.” Resilience isn’t about short-term adjustment or “bouncing back” to a prior state following disruption; it is about being able to nimbly adapt in an ongoing dynamic business environment. The underlying assumption in resilient operation is that volatility in the utility sector will persist. Hence, it is vital to have the talent, capabilities, techniques, operational processes, architecture, tools and applications to constantly and dynamically adapt to evolving business patterns.
- **Technology Capabilities Enabling Resilience.** The three trends aligned to this opportunity show promise in resolving key challenges associated with out-of-date technologies and architectures. They also create opportunities to offer new products and services and support business model transformation. The global drive toward sustainability puts emphasis on new forms of energy generation that produce less pollutants, such as hydrogen and renewables. Though they have less impact on the environment, they create challenging operating conditions for utilities by reducing controllability of the supply and impacting reliability of the delivery infrastructure, subsequently increasing overall business volatility. To address those challenges, utilities have to invest into new capabilities, such as decision intelligence. However, it also means organizations must be composable with modular, adjustable and autonomous components. They must use technologies and leverage technology domain integration to achieve sustained resilience. Business and IT processes must be automated – and digitalized, in particular – when it comes to work and asset operations.
- **Evolving Utility Customer.** The three trends aligned to this opportunity show promise in resolving key challenges, as well as capturing opportunities created by changing needs of technology-empowered and sustainability-driven customers. Democratization of energy provisioning and increased awareness of water customers on resource scarcity forces utilities to change their value proposition to a customer base that is environmentally aware and sustainability awakened. Providing new products and services to customers focused on reducing their carbon footprint, engaging prosumers and their contribution to energy balancing and grid firming needs requires new means of digital customer engagements. At the same time, utilities should not forget their social obligation and their key tenet to provide affordable, accessible and acceptable energy and water to all customers.



## Document Revision History

Research Roundup: Top 5 Business Trends Shaping the Utility Sector in 2022 - 28 January 2022

---

## Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

[Infographic: Top Priorities, Technologies and Challenges in Utilities for 2023](#)

[2022 Strategic Roadmap for Composable Utility Customer Information Systems](#)

[2022 Strategic Roadmap for Asset Management](#)

[Predicts 2023: Adapting to the Energy Transition](#)

[Hype Cycle for Utility Industry IT, 2022](#)

[Hype Cycle for Digital Grid Transformation Technologies, 2022](#)

[Hype Cycle for Disruptive Energy Technologies, 2022](#)

[Digital-Outcome-Driven Metrics for Utilities](#)

---

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

**APPENDIX D**  
**ILLUSTRATION OF IT PROJECT LIFECYCLE**

- Appendix D – IT Project Lifecycle (PAO-SDG&E-043-LMW – see Q1.E)

**Data Request Number: PAO-SDGE-043-LMW**

**Proceeding Name: A2205015\_016 - SoCalGas and SDGE 2024 GRC**

**Publish To: Public Advocates Office**

**Date Received: 8/22/2022**

**Date Responded: 9/6/2022**

1. Regarding the capital projects identified in the attached table please provide the following information:

<b>Capital Project and Category (in \$000's)</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>
00920AI RAMP Fld. Del. Schedule – Cat. C	13,400	10,437	13,206
00920T RAMP Fld. Del. Platform – Category C	0	3,402	6,090
218810 Smart Meter 2.0 – Category C	4,292	32,802	58,459
00903E CIS Reg. Enhance 2022 – Category D	19,233	0	0
00903F CIS Reg. Enhance 2023 – Category D	0	19,752	0
00903G CIS Reg. Enhance 2024 – Category D	0	0	23,768
00903B Contact Center of Future – Category D	0	11,285	9,789
00920BL RAMP Elec Dist Asset – Category M	3,314	5,694	3,731
00920BM RAMP Asset 360 – Category M	4,389	4,269	2,347
00920E Investment Priority – Category M	1,873	5,502	9,256
00907N Microsoft Agreement – Category O	27,900	0	0
00908X RAMP Cloud Foundations – Cat. O	5,968	4,812	5,312
00925I-K RAMP TCRI 2022-2024 – Category O	4,413	4,413	4,413
00920AR App Vulnerable – Category O	3,270	4,000	4,000
00925L RAMP LAN Refresh - Category O	3,734	4,245	4,945
00925M RAMP Fan Voice – Category O	10,357	0	0
00920BC RAMP Digital Process – Category O	4,950	4,950	4,853
00900D Smart Meter 2022-2024 – Category O	0	5,460	3,663
00920BD Found. Analytics – Category O	6,642	5,767	5,867
00920P RAMP Digital Asset – Category O	4,505	3,680	3,680

a. Project cost support (inclusive of calculations and support for those calculations) clearly identifying how the amounts for each year (2022, 2023, and 2024) were determined.

**SDG&E Response 1a:**

SDG&E objects to this request pursuant to Rule 10.1 of the Commission’s Rules of Practice and Procedure on the grounds that it is vague and ambiguous to the phrase “Project cost support.” Notwithstanding the objection noted above, for purposes of this data response, SDG&E interprets project cost support as costs broken down between labor and non-labor. Subject to and without waiving this objection, SDG&E responds by answering Question 1a as follows:

SDG&E developed its project cost estimates based on subject matter experts and proprietary vendor input.

Responses to Question 1a can be found in the individual attachment for each project in the table below, identified by the Project Work Paper.

**Data Request Number: PAO-SDGE-043-LMW**

**Proceeding Name: A2205015\_016 - SoCalGas and SDGE 2024 GRC**

**Publish To: Public Advocates Office**

**Date Received: 8/22/2022**

**Date Responded: 9/6/2022**

Project Name	Work Paper	Project Status	If in Execution, what phase is it in?	File Name
RAMP Fld. Del. Schedule (FSD)	920AI	Execution	Requirements/Design	PAO-SDGE-043-LMW_SDGE-25_920AI_RAMP Fld. Del. Schedule-FSD
RAMP Fld. Del. Platform	920T	Concept		PAO-SDGE-043-LMW_SDGE-25_920T_RAMP Fld. Del. Platform
Smart Meter 2.0	218810	Business Case		PAO-SDGE-043-LMW_SDGE-25_218810_Smart Meter 2.0
CIS Reg. 2022	903E	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_903E_CIS Reg. 2022
CIS Reg. 2023	903F	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_903F_CIS Reg. 2023
CIS Reg. 2024	903G	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_903G_CIS Reg. 2024
Contact Center of the Future	903B	Concept		PAO-SDGE-043-LMW_SDGE-25_903B_Contact Center of the Future
RAMP Elec Dist Asset	920BL	Execution	Implementation	PAO-SDGE-043-LMW_SDGE-25_920BL_RAMP Elec Dist Asset
RAMP Asset 360	920BM	Execution	Implementation	PAO-SDGE-043-LMW_SDGE-25_920BM_RAMP Asset 360
Investment Priority	920E	Execution	Requirements/Design	PAO-SDGE-043-LMW_SDGE-25_920E_Investment Priority
Microsoft Agreement	907N	Concept		PAO-SDGE-043-LMW_SDGE-25_907N_Microsoft Agreement
RAMP Cloud Foundations	908X	Execution	Implementation	PAO-SDGE-043-LMW_SDGE-25_908X_RAMP Cloud Foundations
RAMP TCRI 2022	925I	Execution	Implementation	PAO-SDGE-043-LMW_SDGE-25_925I_RAMP TCRI 2022
RAMP TCRI 2023	925J	Concept		PAO-SDGE-043-LMW_SDGE-25_925J_RAMP TCRI 2023
RAMP TCRI 2024	925K	Concept		PAO-SDGE-043-LMW_SDGE-25_925K_RAMP TCRI 2024
App Vulnerable	920AR	Execution	Build/Testing	PAO-SDGE-043-LMW_SDGE-25_920AR_App Vulnerable
RAMP LAN Refresh	925L	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_925L_RAMP LAN Refresh
RAMP Fan Voice	925M	Execution	Implementation	PAO-SDGE-043-LMW_SDGE-25_925M_RAMP Fan Voice
RAMP Digital Process	920BC	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_920BC_RAMP Digital Process
Smart Meter 2022-2024	900D	Concept		PAO-SDGE-043-LMW_SDGE-25_900D_Smart Meter 2022-2024
Found. Analytics	920BD	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_920BD_Found. Analytics
RAMP Digital Asset	920P	Execution	Agile	PAO-SDGE-043-LMW_SDGE-25_920P_RAMP Digital Asset

b. Is the project approved by management indicating regardless of the outcome of this instant GRC that the project will be started and completed. Or is the project subject to management discretion and funding, indicating projects may or may not actually be started and completed within this current GRC cycle.

**SDG&E Response 1b:**

SDG&E objects to this request pursuant to Rule 10.1 of the Commission’s Rules of Practice and Procedure on the grounds that it is vague and ambiguous. Subject to and without waiving this objection, SDG&E responds by answering Question 1b as follows:

As described in SDG&E Testimony (Chapter 2, section VI, subsection B) of Tia L. Ballard and William J. Exon (Ex. SDG&E-25) project approval may occur in various phases of the process to identify, develop, and proceed to execution of a project. Similarly, an identified project may not commence execution or achieve completion or may be deferred for various reasons after a Business Case has been approved. Those reasons include, but are not limited to, other competing business priorities, system vulnerabilities, scope changes, internal and vendor resources availability, and management discretion.

**Data Request Number:** PAO-SDGE-043-LMW

**Proceeding Name:** A2205015\_016 - SoCalGas and SDGE 2024 GRC

**Publish To:** Public Advocates Office

**Date Received:** 8/22/2022

**Date Responded:** 9/6/2022

c. Does the project provide any cost savings? If no, then why not? If yes, the amount of savings, support for the calculation of those savings, and where in the current GRC those savings are recognized.

**SDG&E Response 1c:**

SDG&E objects to this request pursuant to Rule 10.1 of the Commission's Rules of Practice and Procedure on the grounds that it is vague and ambiguous as to the definition of "cost savings" and calls for speculation. Subject to and without waiving these objections, SDG&E responds by answering Question 1c as follows:

IT projects are developed to support the Company's operations and capture a variety of benefits for business operations and customers. See SDG&E testimony (Chapter 1, section I, subsection A; Chapter 2, section I, subsection A and C) of Ben W. Gordon, Tia L. Ballard and William J. Exon (Ex. SDG&E-25). By their nature, technology solutions are woven into everyday activities. To the extent savings may be present, any potential savings related to a particular project may be tangible and/or intangible and can range from avoided costs to enablement of business efficiencies. For example, users are forced to leverage less efficient workarounds when services are not available. By providing more reliable technology services, IT enables SDG&E business units to improve their operations rather than being less productive when the systems are not available and ready for their usage.

d. A project timeline showing start date, completion milestones, and completion date.

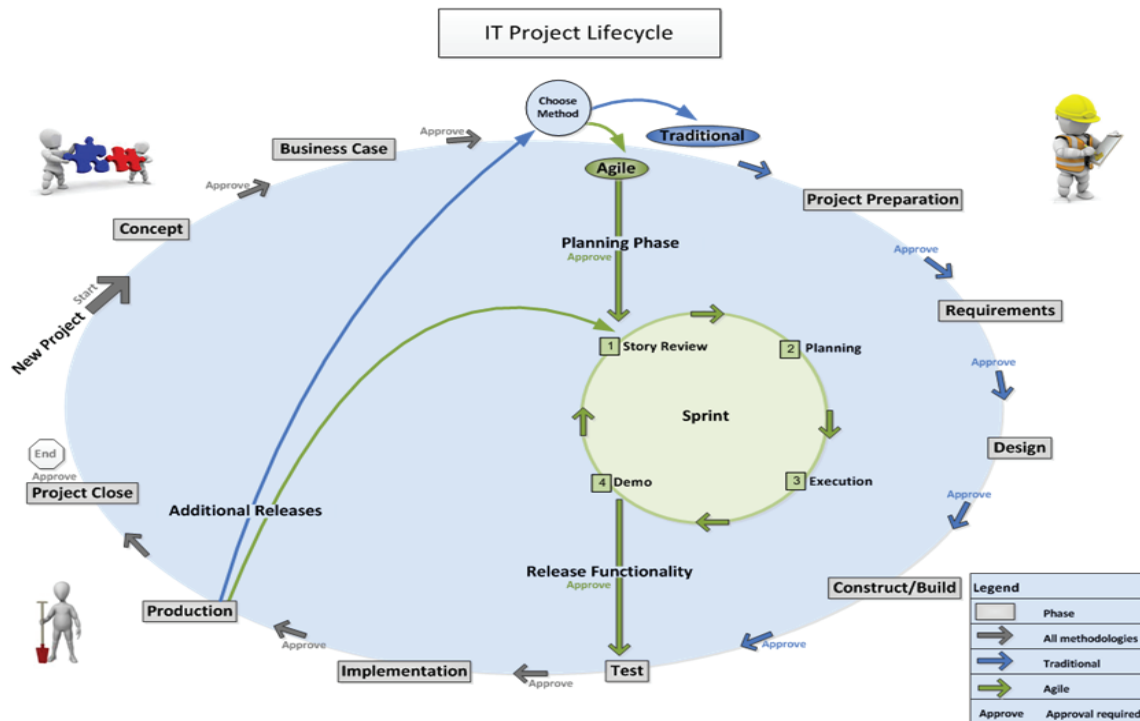
**SDG&E Response 1d:**

The estimated timeline provided for each identified project in response to Question 1d reflects the start date, completion milestones, and completion date where applicable. Please see the Attachment accompanying response to Question 1a for the related project. SDG&E developed its project timeline based on subject matter experts and proprietary vendor input.

e. At what stage is the project in its project life cycle? In providing an answer, please describe SDG&E's project life cycle process, phases, and a description of what each phase means.

**SDG&E Response 1e:**

Please see the “Project Status” field in the table provided in response to Question 1a above. SDG&E further provides the following a visual of the IT Project Lifecycle:



Below are descriptions of the activities that occur in various phases within the IT Project Lifecycle. This agile project timeline is represented in short cycles, as described in the SDG&E testimony (Chapter 1, section I, subsection B) of Ben W. Gordon, Tia L. Ballard, and William J. Exon (Ex. SDG&E-25).

**Concept**

Investigate technology and new business opportunities to recommend whether or not to develop and implement technology products. Provide early high-level analysis of potential solutions, costs, and benefits.

**Business Case**

**Data Request Number:** PAO-SDGE-043-LMW

**Proceeding Name:** A2205015\_016 - SoCalGas and SDGE 2024 GRC

**Publish To:** Public Advocates Office

**Date Received:** 8/22/2022

**Date Responded:** 9/6/2022

Defines the scope of work and total cost of project. The primary purpose of this phase is to provide a detailed analysis to present the business value of a project along with its budget, schedule, and ongoing support requirements.

## **Execution**

### **Project Preparation Phase:**

Complete the preparations necessary to plan and mobilize resources needed for the completion of the project as approved in the Business Case.

### **Requirements Phase:**

Develop detailed requirements to define and document client's needs. Obtain agreement from IT, the requestor(s), and the stakeholders. Define the risks and dependencies and, if necessary, update the estimated effort.

### **Design Phase:**

Develop product design and operating specification in preparation for the Construct/Build Phase. Consider sourcing options Initiate security design. Evaluate the overall design effort for ability to trace requirements and any missing requirements needed to deliver the Business Case.

### **Construct/Build Phase:**

Complete the steps necessary to establish a product which meets client requirement specifications and system design specifications. Complete the deliverables necessary to prepare for testing the product and for training personnel to use and support it.

### **Test Phase:**

Test and verify end-to-end functionality of the product. Verify all requirements are implemented and at an acceptable level of quality. Perform test cases to assure that each component of the product executes without errors.

## **Implementation**

Implement new and enhanced application systems and infrastructure hardware/software into production support environment. Provide storm period support as partnership between project team and production support organizations.

### **Production Phase:**

Provides the baseline service level required to sustain normal operations of the production environment for application and infrastructure hardware and software.

### **Project Closeout:**

Formally close out the project financials (work orders, invoices, etc.), review the project to determine best practices and lessons learned.

**Data Request Number:** PAO-SDGE-043-LMW

**Proceeding Name:** A2205015\_016 - SoCalGas and SDGE 2024 GRC

**Publish To:** Public Advocates Office

**Date Received:** 8/22/2022

**Date Responded:** 9/6/2022

**Agile software development:**

Agile software development refers to a group of software development methodologies based on iterative development, where requirements and solutions evolve through collaboration between self-organizing cross-functional teams.

f. Were any alternatives considered? If no, then why not? If yes, then provide a description of the alternative considered, the cost, and why SDG&E chose not to adopt the alternative.

**SDG&E Response 1f:**

Pursuant to Rule 10.1 of the Commission's Rules of Practice and Procedure, SDG&E objects to this request on the grounds that the request seeks information not relevant to the subject matter involved in the pending proceeding and therefore, the burden, expense and intrusiveness of this request outweighs the likelihood that the information sought will lead to the discovery of admissible evidence. SDG&E also objects on the grounds that it is vague and ambiguous. In particular, this request seeks information concerning costs associated with "alternatives considered." Subject to and without waiving this objection, SDG&E responds as follows answering Question 1(f):

Please see the Attachment accompanying response to Question 1a for the related project for the response to Question 1f.

g. Were any of the project costs subject to competitive bidding? If no, then why not? If yes, then please provide the metrics used and results of the bidding process.

**SDG&E Response 1g:**

Pursuant to Rule 10.1 of the Commission's Rules of Practice and Procedure, SDG&E objects to this request on the grounds that the request seeks information not relevant to the subject matter involved in the pending proceeding and therefore, the burden, expense and intrusiveness of this request outweighs the likelihood that the information sought will lead to the discovery of admissible evidence. In particular, this request seeks information concerning "project costs subject to competitive bidding," "metrics used" and "results of the bidding process." Subject to and without waiving this objection, SDG&E responds as follows answering Question 1(g):

Please see the Attachment accompanying response to Question 1a for the related project for the response to Question 1g.

h. In reference to project 218810 Smart Meter 2.0, were SDG&E's previous Smart Meter projects subject to memorandum account treatment. If yes, what were the reasons for recording the costs to a memorandum account as opposed to inclusion in a GRC?



**Data Request Number: PAO-SDGE-043-LMW**

**Proceeding Name: A2205015\_016 - SoCalGas and SDGE 2024 GRC**

**Publish To: Public Advocates Office**

**Date Received: 8/22/2022**

**Date Responded: 9/6/2022**

**SDG&E Response 1h:**

No. For the previous Smart Meter project (Advanced Metering Infrastructure), SDG&E was subject to balancing account treatment, as described in Advice Letter 1897-E/1693-G and D.07-04-043.

i. In reference to RAMP projects, are all the RAMP projects absolutely started and completed as forecasted in a GRC? Or are RAMP projects subject to management discretion and funding indicating projects may or may not actually be started and completed within a GRC cycle?

<b>Capital Project and Category (in \$000's)</b>	<b>2022</b>	<b>2023</b>	<b>2024</b>
00920AI RAMP Fld. Del. Schedule – Cat. C	13,400	10,437	13,206
00920T RAMP Fld. Del. Platform – Category C	0	3,402	6,090
218810 Smart Meter 2.0 – Category C	4,292	32,802	58,459
00903E CIS Reg. Enhance 2022 – Category D	19,233	0	0
00903F CIS Reg. Enhance 2023 – Category D	0	19,752	0
00903G CIS Reg. Enhance 2024 – Category D	0	0	23,768
00903B Contact Center of Future – Category D	0	11,285	9,789
00920BL RAMP Elec Dist Asset – Category M	3,314	5,694	3,731
00920BM RAMP Asset 360 – Category M	4,389	4,269	2,347
00920E Investment Priority – Category M	1,873	5,502	9,256
00907N Microsoft Agreement – Category O	27,900	0	0
00908X RAMP Cloud Foundations – Cat. O	5,968	4,812	5,312
00925I-K RAMP TCRI 2022-2024 – Category O	4,413	4,413	4,413
00920AR App Vulnerable – Category O	3,270	4,000	4,000
00925L RAMP LAN Refresh - Category O	3,734	4,245	4,945
00925M RAMP Fan Voice – Category O	10,357	0	0
00920BC RAMP Digital Process – Category O	4,950	4,950	4,853
00900D Smart Meter 2022-2024 – Category O	0	5,460	3,663
00920BD Found. Analytics – Category O	6,642	5,767	5,867
00920P RAMP Digital Asset – Category O	4,505	3,680	3,680

**SDG&E Response 1i:**

SDG&E objects to this request on the grounds that it calls for speculation. Subject to and without waiving the foregoing objections, SDG&E responds as follows:

Please see the objections and response to Question 1b.

2. In relation to SDG&E's previous GRC A.17-10-007, were all the capital projects contained within SDG&E's information technology workpapers started and completed as forecasted? If no, please provide a comparative exhibit (by project and by year) indicating the projects forecasted in the previous GRC, and their representative forecasted amount as compared to the actual projects started and completed and the costs of those projects. Within the comparative exhibit, please identify those projects (although