Application: A.18-11-015

Exhibit No.: SDG&E-

Witness: Tom Moses

UPDATED PREPARED DIRECT TESTIMONY OF

TOM MOSES

CHAPTER 3

ON BEHALF OF SAN DIEGO GAS & ELECTRIC COMPANY

BEFORE THE PUBLIC UTILITIES COMMISSION
OF THE STATE OF CALIFORNIA

NOVEMBER 13, 2020

TABLE OF CONTENTS

UPDATED PREPARED DIRECT TESTIMONY OF TOM MOSES - CHAPTER 3

I. INTRODUCTION

The purpose of my updated prepared direct testimony is to provide an update and supersede the prepared direct testimony filed on November 26, 2018 by Claudio Pellegrini, which is necessitated by the passage of time that has elapsed since the Application and testimony was originally filed.[1] In that initial testimony, Mr. Pellegrini provided the technical perspective and cost estimates, where needed, of the following items, in order of appearance in Resolution E-4868 (August 24, 2017) ("Resolution"), in Ordering Paragraph ("OP") 29.[2] My testimony will include:

(1) a cost estimate for Application Programming Interface ("API") Solution 1;

(2) a discussion of the requirement for synchronous data of the complete and expanded data set within ninety seconds;

(3) a cost estimate and proposal for upgrades to the Information Technology ("IT") infrastructure needed for the click through authorization process ("CTP");

(4) a cost estimate and proposal for additional functionalities for the CTP proposed by stakeholders in the Customer Data Access Committee ("CDAC"); and

(5) a cost estimate and proposal for additional functionalities for CTP by San Diego Gas & Electric Company ("SDG&E").

[1] This update testimony has been authorized by the Assigned Commissioner's First Amended Scoping Memo and Ruling (October 23, 2020) at 6.

[2] *See* Resolution, OP 29 at 105-106, bullets 2, 3, 5,6 and 7. The Updated Prepared Direct Testimony of Douglas White (Chapter 1) ("White Testimony (Chapter 1)") and the Updated Prepared Direct Testimony of Neil Umali (Chapter 2) ("Umali Testimony (Chapter 2)") address bullets 4, 8 and 10. Bullet 1 was removed from the scope of this Application by the Assigned Commissioner's First Amended Scoping Memo and Ruling (October 23, 2020), and will therefore not be addressed in my testimony.

My prepared direct testimony focuses on IT impacts, timelines, costs and resourcing of the OP 29 elements. Witness Neil Umali (Chapter 2) discusses the business impacts, timelines, costs and resourcing of the same items.[3]

II. CURRENT BUSINESS FUNCTIONALITY

A. Current Overview on CTP

This section provides an overview of the existing functionality for SDG&E's CTP. As required by the Resolution, SDG&E's CTP[4] was implemented by SDG&E in three phases with the first phase implemented in March of 2018, and the third phase concluding in November 2018 at the time of the original application. Table TM-1, below, reflects the elements implemented in each phase of SDG&E's CTP.

Table TM-1: Phases and Functionality for Implementation of SDG&E's CTP

Phase	Functionality
Phase 1	• Authentication • Authorization with streamlined design • Demand Response Provider revocation • Design with 2 clicks & 4 screens for best case • Display of Terms & Conditions • Dual Authorization • Length of authorization options. • Mobile friendly design • "Future-Proof" click through architecture
Phase 2	• Alternative Authentication • Expanded Data Set • Performance monitoring/reporting • Shorter Data Set Synchronously
Phase 3	• Complete Expanded Data Set Synchronously • Revocation using click through authorization

[3] *See* Umali Testimony (Chapter 2).

[4] The Resolution refers to Solutions 1, 2 and 3. Solution 3 is SDG&E's current CTP.

SDG&E's CTP solution offers a wide breadth of functionality, including: (1) the flexibility for a Demand Response Provider ("DRP") to provide their own preferences for how long a customer's data sharing authorization must last; (2) the ability for DRPs to easily choose the scope of data they would like to receive; (3) the ability for SDG&E customers to easily authenticate with SDG&E prior to authorizing the sharing of their data, either by logging in with credentials they have familiarity with, such as their SDG&E My Account credentials or via alternate authentication, where they can demonstrate their customer relationship with SDG&E; (4) the ability for SDG&E customers to authorize the sharing of their customer data with a DRP, including the duration and service accounts for which they would like to share data; and (5) the ability for SDG&E customers to view past and current data sharing authorizations, and revoke them when desired.

From a technology perspective, the CTP leverages industry best practices to enable these features. This is done using widely-known industry standards, including but not limited to, a framework called Open Authorization ("OAuth"). OAuth is an industry-standard template for designing authorization flows for web applications, desktop applications, mobile phones, and in-home devices. The framework is developed as an RFC ("Request For Comment") document[5] and documented by the IETF OAuth Working Group in their standards track.[6] The IETF represents an international community of working groups made up of designers, vendors, and operators intent on promoting standards for the proper use, implementation, and adoption of the

[5] An RFC is a type of publication from the technology community. RFCs may come from many bodies including from the Internet Engineering Task Force ("IETF"), the Internet Research Task Force ("IRTF"), the Internet Architecture Board ("IAB") or from independent authors.

[6] The OAuth 2.0 Authorization Framework is published by the IETF as a RFC document. *See* Internet Engineering Task Force, *The OAuth 2.0 Authorization Framework* (October 2012) ("IETF OAuth 2.0"), *available at* https://www.rfc-editor.org/rfc/rfc6749.txt

internet by publishing protocol standards, current best practices, and technical documents related to those standards. This intent is documented as part of the IETF's Mission Statement.[7] SDG&E aligns its system implementations to IETF standards as well as those of other standards bodies.[8]

As an industry standard, OAuth ensures that the act of authorizing access to data is done securely and uses a consistent approach. The standard also covers the definitions of various actors or roles that typically partake in a data sharing transaction and provides guidance as to how those roles should be separated so that trust in the data sharing transaction is established. Those roles are: (1) the role of the party owning the data, *i.e.*, a SDG&E customer; (2) the role of the party mediating the sharing of data, *i.e.*, SDG&E; and (3) the role of the party requesting the data, *i.e.*, a DRP. When the OAuth framework is implemented correctly and the roles are properly separated,[9] the result is that (1) SDG&E customers can trust that SDG&E will only provide data to a DRP when the customer has authorized it; (2) SDG&E customers can trust that DRPs cannot obtain the data on their own when the customer has not authorized them to receive it; and (3) the scope of the data the customer authorizes is the same scope of data that the DRP is allowed to receive and not a different one. The CTP implements this framework correctly and therefore abides by the OAuth standard.

[7] *See* H. Alvestrand, *A Mission Statement for the IETF* (October 2004), p.1, *available* at https://www.rfc-editor.org/rfc/rfc3935.txt

[8] SDG&E aligns its systems implementations to other industry standards bodies such as the National Institute of Standards and Technology ("NIST"), the Open Web Application Security Project ("OWASP"), and the World Wide Web Consortium ("W3C") for internet standards.

[9] The concept of separating roles in the OAuth framework is intended to prevent fraud and to ensure that no role has too much responsibility assigned to it.

B. Current CTP Adoption and Performance

SDG&E's overall assessment of the CTP is that it continues to achieve what it was intended to achieve. From an adoption and performance perspective, the current CTP performance metrics show that the CTP is not only being actively adopted by DRPs and SDG&E customers but that the CTP is performing efficiently. SDG&E began collecting performance metrics as specified by the Resolution at the beginning of September 2018. The following metrics[10] represent CTP adoption and performance:

1. For the past three months, the average time it takes to load a web page on the CTP is approximately 3 seconds.
2. SDG&E customers have submitted over 29,000 authorizations using the CTP between July 2018 and October 2020.

SDG&E believes these metrics demonstrate strong CTP performance during the first twenty seven months of CTP operations.

III. SYNCHRONOUS DATA OF THE COMPLETE AND EXPANDED DATA SET WITHIN 90 SECONDS

A. CTP Data Set Performance

Per Resolution OP 18, SDG&E was ordered to propose the delivery of a smaller synchronous data set to DRPs within 90 seconds. As a result, SDG&E filed Advice Letter E-3136, which was approved by Resolution E-4194, and which provided evidence that SDG&E could meet this requirement. The evidence showed that SDG&E could deliver the CTP current data set[11] with response times under 90 seconds, averaging under half a second. Table TM-2, below, represents more up to date performance metrics showing that SDG&E is still able to meet this requirement today in the CTP.

[10] *See* Resolution, OP 21 and p.54 for discussion on stakeholder proposed metrics.

[11] *See* Resolution, Attachment 1.

Table TM-2:
CTP Synchronous Data Set Performance - September 2020

Service Name	Timeframe	Number of Invocations July 2020	Number of Invocations August 2020	Number of invocations September 2020	Average Response Time
Customer Account Overview Service	07/1/2020 to 09/23/2020	~2,255	871	589	~ 574 milliseconds
Enterprise Energy Usage Service	07/1/2020 to 09/23/2020	~9,841	9,957	9,966	~179 milliseconds
Program Participation Service		0[12]	0	0	Not applicable
Customer Authorization Search Service	07/1/2020 to 09/23/2020	~2,343	878	591	~272 milliseconds
Customer Authorization Create Service	07/1/2020 to 09/23/2020	~2,099	793	418	916 milliseconds
Billing Service		0	0	0	Not applicable

B. Cost Estimates

Based on the sub-second performance of services indicated above, SDG&E is confident no additional costs are required to continue meeting the 90-second requirement for the current data set.

IV. UPGRADES TO THE INFORMATION TECHNOLOGY INFRASTRUCTURE NEEDED FOR THE CTP (OP 29, BULLET #6)

A. CTP Infrastructure Upgrades

SDG&E is anticipating more DRP integration testing[13] will be needed in the future as more DRPs adopt the CTP. SDG&E expects that a dedicated test environment will be needed to ensure that DRPs can quickly integrate and test the CTP after they register with SDG&E.

[12] The CTP performance metrics reported that the program participation service and the billing service were not accessed by any DRPs in the third quarter of 2020.

[13] Upon successful registration with SDG&E, DRPs are required to build integration and test, in order to successfully access the data set offered with the CTP.

SDG&E proposes new integration test environments for key systems used by the CTP. From a technical perspective, this involves provisioning new physical hardware (servers)[14] as required, installing software on them and connecting them to the CTP.

B. Cost Estimates

Table TM-3, below, represents the capital cost estimates to install the test environments described above as part of a three-month project. These costs represent all phases of the project including requirements elicitation, design, build, test, and implementation. Non-labor costs represent the use of vendor professional services to provide test environments as described. Labor costs represent the use of internal SDG&E resources to provide technical consultation, project management, and business systems analysis services to the vendor during those same phases of the project.

Table TM-3:
Capital Integration Environment Build/Implementation Cost Estimates

	Labor (dollars)	Non-Labor (dollars)	Total Duration (months)
System Test Environment	$17,373	$36,203[15]	3

Table TM-4, below, represents the costs to maintain and make this functionality available over an operational period of three years, for example, supporting the operation of the computing infrastructure, including hardware (*e.g.* servers to storage systems), and software (*e.g.* middleware, production control, operating systems, and other low-level software systems). SDG&E is requesting budget for these estimates. SDG&E proposes to recover ongoing costs

[14] A server is a physical chassis containing several central processing units, memory cards, and hard drives to provide computing resources to a network.

[15] Includes costs to provision a new virtual private cloud environment.

associated with the CTP. This cost recovery proposal is discussed in the prepared direct testimony of Clare Olegario (Chapter 6).

Table TM-4:
Integration Environment Operational Cost Estimates

	Labor (dollars)	Non-Labor (dollars)	Total Duration (months)
System Test Environment	$0	$31,383[16]	36

These requested budgets are included in Table DW-1 found in the prepared direct testimony of Douglas White (Chapter 1) ("White Testimony (Chapter 1)") and are included in the revenue requirement discussed in the prepared direct testimony of Kristi Khong (Chapter 5) ("Khong Testimony (Chapter 5)").

V. ADDITIONAL FUNCTIONALITIES FOR CTP PROPOSED IN THE CDAC (OP 29, BULLET #7)

The following items are third-party requested enhancements to the CTP through the CDAC. Some of these improvements are applicable for SDG&E and discussion is included below for each pertinent item to explain how SDG&E would address these enhancements. My prepared direct testimony does not discuss requested enhancements that are already implemented in SDG&E's CTP.[17] The Umali Testimony (Chapter 2) describes each of the requests for CTP enhancements that were received by SDG&E and whether the enhancement requests will be accommodated. The requested enhancements provided by stakeholders, include:

1. Improvements to ongoing data delivery;[18]
2. Functionality to inform the authorized provider with details on the status of the customer authorization;

[16] The non-labor costs include licensing costs required to provision a test environment.

[17] *See* Umali Testimony (Chapter 2), Section III. Click-Through Authorization Enhancements.

[18] These improvements included a request for SDG&E to correct gaps in interval data, send interval data on a timelier basis, within a period of an hour up to a day, and allow DRPs to re-request interval data.

3. Use of SDG&E's company logo on the third-party website to identify where a SDG&E customer would initiate the CTP;

4. Specific enhancement to the sign-in page providing sign-up for an online account or retrieval of credentials;

5. Functionality to facilitate resolution of enrollment conflicts as an optional part of the click through flow;

6. Improved visibility into why a customer fails to complete the OAuth process;

7. Lengthen lifespan of the refresh tokens to at least one year; and

8. Transition of the revocation notification from email to a file (or push notification);

These requested enhancements to IT applications are discussed in detail below.

A. Improvements for on-going data delivery

Both the Resolution and DRPs sought on-going data delivery improvements.[19] In its initial CTP roll-out, SDG&E implemented significant functionality to offer on-going data delivery to DRPs. Based on feedback to date, there are no further enhancements required for on-going data delivery capabilities . For example, today SDG&E proactively sends DRPs interval data corrections as part of the regularly transmitted update file.

Additionally, DRPs can request corrective files at any time using an automated web service process and those corrective requests will usually be processed by SDG&E within 3 hours from the time they are received. Moreover, once a customer initially authorizes a DRP to receive historical interval data that data typically starts flowing to the DRP within a few hours. SDG&E maintains an automated process that sweeps for new customer authorizations every 15 minutes. Once a new authorization is detected, the process to retrieve, assemble, and send historical interval data to a DRP starts immediately.

Given the above, the data delivery process provided by SDG&E is adequate.

[19] *See* Resolution, OP 29 at 105, bullet 5.

B. Functionality to inform the authorized provider with details on the status of the customer authorization

SDG&E was also asked to consider "functionality to inform the authorized provider with details on the status of the customer authorization."[20] SDG&E already offers details of a customer's authorization as part of the current CTP data set. However, the data set does not provide the status of the authorization. In situations where the DRP stops receiving customer data, the status within the data set can provide the DRP the ability to determine if the authorization was revoked, cancelled or expired. SDG&E will include the functionality by enhancing the CTP to include the ability to retrieve status of the customer's authorization, this enhancement also resolves issue number 8 above: Transition of the revocation notification from email to a file (or push notification).

C. Functionality to facilitate resolution of enrollment conflicts as an optional part of the click through flow

SDG&E proposes an enhancement to the authorization screen of the CTP that will inform the customer if they are participating in one or more SDG&E Demand Response programs. This CTP enhancement serves to prevent program enrollment conflicts early in the process, which is when the customer is preparing to consent. This enhancement serves to improve the customer's and DRP's experience of the CTP by advising them of potential conflicts when authorizing.

From a technical perspective, this enhancement would require that the CTP be integrated to additional systems giving it the ability to determine if program enrollment conflicts exist. Today, other program enrollment conflict checks occur downstream in SDG&E's Rule 32 automation when SDG&E receives DRP location registrations from the California Independent

[20] *See* OhmConnect, *Proposed Enhancements to the OAuth Click-Through Solution*, June 2018, slide 2, item 2.

System Operator ("CAISO").[21] This enhancement serves to further improve the overall experience for DRPs using the CTP by identifying conflicts early and often, thus saving them time.

D. Cost Estimates of Enhancements Proposed in the CDAC

Table TM-5A, below, represents the costs to build and implement the CTP enhancements proposed in the CDAC as part of a four-month project. The costs include all phases of that project such as requirements elicitation, design, build, test, and implementation. Non-labor costs represent the use of vendor professional services to provide the enhancements as described. Labor costs represent the use of internal SDG&E resources to provide technical consultation services, project management, and business systems analysis to the vendor during requirements elicitation, design, build, test, and implementation phases of the project.

Table TM-5A:
Capital CTP Enhancements Proposed in CDAC – Build/Implementation Costs

	Labor (dollars)	Non-Labor (dollars)	Total Duration (months)
Status of Authorization	$46,207	$105,740	3
DR Program Eligibility Check	$107,816	$246,726	4

Table TM-5B, below, represents the costs to operationally maintain the CTP enhancements proposed in the CDAC and make them available up to a period of five years. Examples of this type of maintenance include: (1) configuring new DRPs in SDG&E's OAuth framework; (2) supporting integration testing for DRPs; and (3) monitoring the synchronous data set to ensure that its performance continues to be adequate. The maintenance of program

[21] Customers cannot be enrolled in more than one DR program that is bid into the CAISO. The Rule 32 automation handles these conflicts generally.

participation and program eligibility rules is also considered to be an IT function. These costs are included in SDG&E's total budget request and in its revenue requirement discussion.

Table TM-5B:
O&M CTP Enhancements Proposed in CDAC Operational Support Costs

	Labor (dollars)	Non-Labor (dollars)	Total Duration (months)
Status of Authorization	$65	$12,372	36
DR Program Eligibility Check	$151	$28,869	36

SDG&E is requesting these costs as budgets for this operations and maintenance work. These budgets are included in the total budget table found in the White Testimony (Chapter 1), and the Khong Testimony (Chapter 5) as they are included in SDG&E's requested revenue requirement.

VI. CDAC WHITEPAPER RESPONSES

The Umali Testimony (Chapter 2) contains discussion, background, and responses to the requests for enhancements that resulted from the CDAC Whitepaper on Data Access ("Whitepaper"). [22] In his prepared direct testimony, Mr. Umali (Chapter 2) describes each of the requests for CTP enhancements that were received by SDG&E, and whether SDG&E will accommodate those requests. My prepared direct testimony includes the technical perspective and cost estimates for those requests that SDG&E believes should be accommodated.

Currently, SDG&E provides DRPs with the data set that was previously approved by the Resolution[23] and which includes (1) customer data; (2) demand response program participation data; (3) billed consumption data; and (4) interval data. The current data set is offered in two

[22] *See* Umali Testimony (Chapter 2), Section IV. Whitepaper Responses: Requests for Additional Data – Recommended, which discusses the Whitepaper response.

[23] *See* Resolution, OP 19 at 102.

styles: (1) as a synchronous data set, which can be accessed by DRPs to receive authorized customer data immediately; and (2) as an update file containing any changes to authorized customer data, and which is sent to DRPs on a regular basis.

SDG&E proposes expanding the current data set to newly include (1) customer gas interval data, if applicable, based on a customer's service commodities; (2) the customer's last twelve months of rates for the current meter and notification of rate changes; and (3) the customer's historical energy efficiency program participation.

This new, expanded data set would be provided to all current and future DRPs as part of the CTP. From a technical perspective, no major system changes are required to make this happen. However, there are small needed changes for the items described below.

A. Gas Usage Data

SDG&E proposes to provide the customer's monthly aggregated and billed gas consumption. Adding visibility into a customer's gas usage data allows DRPs to more completely understand a customer's energy consumption profile across all of their commodities and determine if energy saving opportunities exist for their therm[24] consumption. SDG&E agrees to include gas interval data in the new expanded data set. This data would be provided where a customer has a communication module installed on their smart gas meter as that module allows the meter to communicate daily gas intervals to SDG&E. The gas usage data will be integrated into the CTP process.

B. Historical Energy Efficiency Program Participation

SDG&E proposes including historical energy efficiency program participation in the expanded data set as this data point can be helpful in evaluating customers for participation in

[24] A therm is a measurement unit representing 100 cubic feet of natural gas.

DRP programs. From a technical perspective, SDG&E proposes enhancing the current CTP data set to allow a DRP to receive a customer's energy efficiency data. This data would also be included as part of the regular update file mentioned above that DRPs receive today, and which would update them when relevant changes occur in a customer's energy efficiency program participation. Both the update files and the synchronous data set would only reflect historical energy efficiency program participation if a customer has been successfully qualified and paid under an energy efficiency program.

C. Last twelve months of rates and notification of rate changes

SDG&E proposes expanding the data set to include a customer's last twelve months of applicable electric and gas rates. From a technical perspective, the CTP currently sends customer billed consumption data. The CTP will be enhanced to integrate with the source systems that provide the customer's historical rate information as well.

D. Cost Estimates

Table TM-6A, below, represents the costs to implement the proposed enhanced functionality discussed above over the course of a seven-month project. The costs include all phases of that project such as requirements elicitation, design, build, test, and implementation. Non-labor costs represent the use of vendor professional services to enhance the current expanded data set as described. Labor costs represent the use of internal SDG&E resources to provide technical consultation services, project management, and business systems analysis to the vendor during requirements, design, build, test, and implementation phases of the project.

Table TM-6A:
Capital Cost Estimates for Build/Implementation to Enhance Expanded Data Set

	Labor (dollars)	Non-Labor (dollars)	Total Duration (months)
Expanded Data Set	$126,291	$375,124	7

Table TM-6B, below, represents the costs to maintain and make this functionality available over an operational period of three years. Examples of this type of maintenance include: (1) configuring new DRPs in SDG&E's OAuth framework; (2) supporting integration testing for DRPs; and (3) monitoring the synchronous data set to ensure that its performance continues to be adequate. These costs are included in SDG&E's total budget requests and revenue requirements.

Table TM-6B:
O&M Cost Estimates for Ongoing Operational Support of Enhanced Expanded Data Set

	Labor (dollars)	Non-Labor (dollars)	Total Duration (months)
Expanded Data Set	$0	$74,702	36

SDG&E is requesting these costs as budgets for this work. These budgets are included in the total budget table found in the White Testimony (Chapter 1) as well as the Khong Testimony (Chapter 5).[25]

VII. ADDITIONAL FUNCTIONALITIES FOR CTP PROPOSED BY SDG&E

A. New Third-Party Communication Process for Planned / Unplanned System Outages Affecting the CTP

SDG&E has implemented a formal communication process to advise DRPs using the CTP when planned or unplanned system outages occur that affect the availability of the platform. The benefit resulting from this communication process is simply increased awareness by DRPs when there are known impacts to the SDG&E CTP they are using. This item is discussed further in Mr. Umali's testimony (Chapter 2).[26]

[25] *See* White Testimony (Chapter 1), Table DW-1, and Khong Testimony (Chapter 5), Section II. Revenue Requirement.

[26] *See* Umali Testimony (Chapter 2), Section III. Click-Through Authorization Enhancements.

B. Future Proofing CTP

SDG&E proposes several approaches that will benefit the CTP and make it more resilient against future changes.[27] All of the approaches discussed in the sub-sections below explain the direct benefit of allowing the CTP to scale effectively and help address the growing demand for customer data by DRPs. They are solely discussed here to give the California Public Utilities Commission ("Commission") an awareness of what SDG&E is already doing to ensure that the CTP continues to effectively serve SDG&E's customers and DRPs into the foreseeable future.

1. Buy vs. Build

SDG&E currently enables part of its customer authorization capabilities via vendor software that it purchased and licensed and that offers OAuth capabilities. The decision to buy the OAuth capabilities, versus building them in-house, offers several benefits to future proof the CTP:

1. Allows the CTP to use the latest version of the OAuth standard through vendor updates;
2. Prevents technology obsolescence through vendor updates; and
3. Ensures appropriate technical security through vendor security patches.

These benefits ensure that the CTP stays secure, technically relevant, interoperable with other vendor technologies, and continues to align to the OAuth standard over time.

2. Data Set Versioning

SDG&E is implementing the concept of versioning on its data set to prevent third-party implementations from breaking when SDG&E makes a change to the data set. This approach eliminates disruption to DRP operations and provides DRPs with the flexibility to adopt the new version of the data set when released, or to continue to utilize the former version.

[27] Resolution OP 23 requires the investor-owned utilities ("IOU") to "future-proof" the CTP authorization solution. *See* Resolution, at 103.

3. Configuration vs. Customization

The difference between configuration and customization is that the configuration takes advantage of the built-in flexibility of an application's software, allowing SDG&E to change predefined settings and make an application function a certain way. Customization involves altering the code of the software itself and is a maintenance approach that takes more time and effort. SDG&E follows a configuration approach for the CTP. This approach has the benefit of allowing SDG&E to roll out enhancements and fixes to the platform much quicker than if it must constantly maintain tens or hundreds of lines of software code each time a change to the platform is required.

4. Automation

The approach of automating business processes has the benefit of providing consistency and making business processes less manual and error-prone. As an example, the CTP uses automation in the on-going data delivery mechanism as well as in the creation of customer authorizations, which saves time and effort for DRPs, SDG&E's customers and SDG&E.

5. One Data Set for All Third Parties

As discussed above, SDG&E intends to offer the same comprehensive and expanded data set to all future DRPs leveraging the CTP. This reduces complexity and allows the CTP to scale effectively irrespective of DRP demands for data.

C. Cost Estimates

SDG&E has already implemented the functionality discussed above and believes it is contributing to the effectiveness of the current CTP. SDG&E seeks no additional funding for these enhancements.

VIII. COST ESTIMATE FOR ALTERNATE SOLUTION (OP 29, BULLET #2)

A. Background

This section discusses the alternate proposal to the CTP, including its genesis, the distinctions between Solution 1a and Solution 1b, and security gaps related to each solution.

During the click-through workshop held on October 5, 2016, the DRPs, with the support of interested parties, and the IOUs, proposed three potential solutions to meet their needs based on the guiding principles each party proposed. Proposed Solution 2 was immediately ruled out, leaving Solutions 1 and 3 to explore further.[28] In an Informal Status Report[29] filed by Pacific Gas and Electric Company ("PG&E") to the DRPs and the Commission, API Solution 1 was described as:

> The customer would begin on the third party DRP site and provide specific customer information via a browser that is sent directly to the utility. The information would be authenticated by the utility's back-end systems. Once authenticated, the customer would authorize release of data on the DRP site and the parameters would be sent to the utility to complete the process. The authentication and authorization steps could, at the option of the DRP, be completed on a single screen. The customer does not leave the DRP website during this process; however, this solution requires the utilities to build one, or possibly two, custom API endpoints to authenticate the customer's identity and authorization of data release to the DRPs.[30]

[28] Solution 1 is referred to as the API Solution or for purposes of my prepared direct testimony, the Alternate Solution, and Solution 3 is referred to as the OAuth Solution. The OAuth Solution is currently in place and operating.

[29] *See* Application 14-06-002, cons., Status Report Ordered by the Assigned Commissioner's Office During Discussions at the October 5, 2016 Click-Through Workshop (October 12, 2016) ("Status Report").

[30] *Id.*, Status Report, Attachment at 1.

The IOUs identified several security concerns with API Solution 1, particularly the ability for DRPs to view and store customer credentials on their systems. The IOU concerns are discussed in the same informal status report:

> Authentication and Authorization: Customer provides confidential authentication information on the third party's website, requiring the customer and the utility to trust that the third party's implementation of this solution does not transmit or store this information on third party servers.[31]
>
> * * *
>
> Security: Depending on how login mechanism is implemented by the DRP, the DRP may have visibility to the customer credentials being passed to the utility authentication web service. If the DRP builds the login, they can build it without assuring the utilities of the proper security, and these concerns cannot be mitigated with any guarantees.[32]

The ability for SDG&E to further evaluate the cybersecurity risks of Solution 1 beyond these aspects was not possible at the time due to a lack of detail regarding process design and architecture. This concern was communicated and documented in the same informal status report:

> Security: API Solution 1 has little implementation description and this inherent lack of detail significantly limits the utilities' ability to assess the full scope of cybersecurity risks that utilities, DRPs and customers are exposed to.[33]

Again, at the April 19, 2018 CDAC workshop, PG&E presented security risks and mitigations related to Solution 1. Specifically, PG&E outlined possible approaches that could help minimize the risk of third parties intercepting and storing customer credentials to later submit fraudulent authorizations. These approaches included the use of "two-factor/multi-factor

[31] *Id.*, Attachment at 2-3.

[32] *Id.*, Attachment at 3.

[33] *Id.*, Attachment at 4.

authentication" to strengthen customer authentication and reduce the risk of identity fraud by DRPs.

In May 2018, a DRP stakeholder attempted to define parameters of Alternate Solution 1. By June 3, 2018, parties had split Solution 1 into 1a and 1b but could not reach consensus on which Solution to advocate. Solution 1b used an approach of two factor authentication which was not part of Solution 1 as originally proposed. At the end of the discussion on Solution 1a and Solution 1b, the stakeholders present did not definitively identify which of the two versions of Solution 1 would be preferred by most third parties. SDG&E decided to estimate Solution 1b because it had slightly fewer security concerns and did not give third parties full control over the login mechanism like Solution 1a did.

Despite attempts to mitigate SDG&E's concerns, both Solution 1a and Solution 1b fall far short in establishing a secure and standards-based approach to customer authentication and customer authorization. In compliance with OP 29 of the Resolution, SDG&E provides below a discussion of Solution 1b[34] and a cost estimate should the Commission order SDG&E to replace the current operational CTP with the Alternate Solution. Based on SDG&E's assessment, neither version of Solution 1 are safe to implement. Specifically, there are extensive, identified gaps in both versions' approach to customer authentication and customer authorization, which present with the potential for dire consequences. Unknown consequences pose further risk. The known authentication and authorization gaps are described below.

[34] Due to the lack of third-party consensus of which Solution 1 (a or b) was preferred, SDG&E has selected Solution 1b because it presents slightly fewer security concerns. A comparison of the two versions is discussed earlier in this section *infra*.

B. Authentication Gaps of the Alternate Solution

Both Solution 1a and 1b would allow the customer to authenticate its customer relationship with SDG&E and authorize the sharing of its data with the third-party on the third party's website, and the third-party informs SDG&E that there has been authentication and authorization by a customer. In contrast, using the current CTP protocol, a customer while on the third-party website clicks directly into a SDG&E website to authenticate their identity as a customer and provide authorization to share information with the third-party service provider.[35]

The distinguishing feature between the two Solution 1 versions involves the manner of customer authentication. Solution 1a proposes to provide DRPs with the discretion to manage customer authentication as they see fit and runs the risk of exposing a customer's credentials to those DRPs; Solution 1b proposes an approach for customer authentication using what is often referred to as multi-factor authentication ("MFA"). The proposed use of a MFA makes Solution 1b slightly less problematic from a security perspective, which is why SDG&E further analyzes this proposal below as the Alternate Solution. Multi-factor authentication is a technique that helps protect the web user when they browse the web and is an additional layer of security that customers can enable when accessing personally sensitive data on the web. It can be summarized by saying that it enforces an additional 'check' or verification of the user's identity beyond the usual verification that is typically seen online with a login screen. Applying this MFA technique has the effect of making it harder for bad actors to impersonate an online user, in this case a customer.

[35] This activity in the existing CPT is conducted within the 2 pages and 4 clicks mandated by the Resolution. *See* Resolution, OP 29 at 105-106.

Despite the conceptual benefits that a MFA would typically offer, the MFA approach being proposed as part of the Alternate Solution does not align with industry best practices and offers no real security benefits. SDG&E knows definitively that an implementation of MFA as proposed would create security risks for SDG&E. For MFA usage, SDG&E follows the nationally recognized National Institute of Standards and Technology ("NIST") organization for the industry definition, best practices and guiding principles. The Alternate Solution's proposed implementation of the MFA does not offer any of the protections provided by the industry standard MFA version approved by NIST.

NIST is an industry body founded in 1901 that is now a part of the U.S. Department of Commerce. NIST's cybersecurity and privacy activities provide standards for the global IT industry to centrally align and strengthen the security of the world's digital environment. In 2017 NIST described multi-factor authentication as:

> An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are *something you know*, *something you have*, and *something you are*.[36]

The three factors that NIST references as part of multi-factor authentication can be explained as follows. The 'something you know' factor is the most common and prevalent today. It is typically seen when an online user uses a login and password to authenticate onto a secure website. Another example would be when an individual enters their personal identification number ("PIN") onto an automatic Teller Machine ("ATM") to securely perform a financial transaction to deposit or withdraw cash. Both the password and the PIN are things that

[36] Paul A. Grassi, Michael E. Garcia, James L. Fenton, *NIST Special Publication 800-63-3: Digital Identity Guidelines* (June 2017), at 49 (emphasis included).

the individual, and only that individual should know. An example of the ‘something you have’ factor is when an individual has a debit card or a credit card that identifies them as a customer of a bank. In the scenario described previously, the factor for ‘something you know’ would be considered the PIN and the factor for ‘something you have’ would be the debit card or credit card that the customer uses at the ATM. This use case is the best example of multi-factor authentication today. As shown, it is a relatively common technique which most people rely on every day to confirm their identity as they make purchases or perform financial transactions securely with their financial institutions. The third factor, or ‘something you are’ is most typically explained using techniques such as retinal scans (digital scans of a human eye) or fingerprint scans. These are examples where the unique make up of a human being is used to identify them securely.

When compared to NIST’s definition, the multi-factor authentication approach proposed by the Alternate Solution is by definition, not at all multi-factor authentication for the simple reason that only a single factor of verification is taking place. There is in fact, no other additional authentication, such as a login, happening beforehand. The Alternate Solution proposes merely to verify the customer’s identity by asking the ostensible customer to provide a personal email address they have on record with SDG&E. This is not a safe or secure method to authenticate customers, and further does not follow the first (or any) of the three NIST MFA key principles, which is something the user and only the user knows. An individual’s email address can be easily obtainable via the internet and is not a piece of identifying information that is private and only that user knows.

From an authentication perspective, there is no version of Alternate Solution that is secure unless a strong and trustworthy customer authentication, such as a login, is implemented as the first factor of MFA (*e.g.*, something you know) and complemented by a second customer authentication using a one-time code (*e.g.*, something you have). In sum, the Alternate Solution is not secure because it proposes a non-standard use of MFA, which is not really multi-factor at all.

C. Authorization Gaps of the Alternate Solution

The Alternate Solution proposed was described by its author: Mission:data as leveraging parts of "Solution 3," the current operational CTP which uses OAuth.[37]

However, an implementation of the Alternate Solution would break the current CTP and cause it to no longer align to OAuth given that it shifts the customer's act of authorizing to now occur on the DRP site under the DRP's control without any oversight by SDG&E. Mission:data may refer to the Alternate Solution as being an OAuth solution, but it should be clearly understood that the Alternate Solution cannot possibly be a standard OAuth given the fundamental change in the way the authorization is handled. As discussed above in Section 2, the OAuth specification includes clear guidance on how to establish trust in a data sharing agreement. In the Alternate Solution, trust is not established because the proposal would essentially allow the DRP freedom to retrieve data at will by creating and modifying customer authorizations without any knowledge of the customer or SDG&E. Section 4 of the OAuth standard documented by IETF discusses in technical detail, the recommended negotiation flow[38] required to establish trust in a data sharing agreement.[39]

[37] The description of the Alternate Solution also mentions "access tokens," which are a concept related to OAuth and documented by the IETF as part of the OAuth standard. *See* IETF OAuth 2.0.

[38] *See* IETF OAuth 2.0 at 7-8.

[39] *Id.*, Section 1.2, Protocol *Flow,* discusses the recommended negotiation flow between the resource owner, the authorizing party and the party providing access to data.

The Alternate Solution proposal also fails to align to any of the documented "grant types" that are part of the OAuth specification. Grant types constitute acceptable and documented patterns within the OAuth standard establishing how customer authorization should be safely obtained. There are four grant types in the OAuth standard, with the 'authorization code' grant model being the most common, the most secure and the one that the current CTP uses.[40] In contrast, the Alternate Solution proposes use of the least secure type of grant called the "Resource Owner Password Credentials Grant," *i.e.*, using a PIN instead of the standard's recommended set of customer credentials. This grant type is defined in IETF's documented OAuth standard, which emphasizes special caution when this type of grant is utilized:

> The resource owner password credentials grant type is suitable in cases where the resource owner has a trust relationship with the client, such as the device operating system or a highly privileged application. The authorization server should take special care when enabling this grant type and only allow it when other flows are not viable.
>
> This grant type is suitable for clients capable of obtaining the resource owner's credentials (username and password, typically using an interactive form). It is also used to migrate existing clients using direct authentication schemes such as HTTP Basic or Digest authentication to OAuth by converting the stored credentials to an access token.[41]

In contrast to the Alternate Solution, the current CTP is a standard implementation of OAuth and uses the most secure grant type, the "authorization code" grant model. The CTP remains the most viable and secure customer authentication/customer authorization platform. No alternate solution is needed.

[40] *Id*., Section 1.3.1, *Authorization Code*, discusses this grant type's security benefit on performing an authorization handshake behind the scenes without risking exposing the negotiation to the online user.

[41] *See* IETF OAuth 2.0 at 37-38.

D. Why Standards Matter

The prior sections describe the use of standards for both MFA and OAuth. The use of industry-recognized and sanctioned standards is crucial for the implementation of a click-through process that can be "future proofed" and is flexible for future expansion, as the Commission has expressed.[42] A CTP proposal that implements either MFA-like or OAuth-like approaches in a non-standard manner should be rejected by the Commission.

The importance of following known and tested industry standards and guidelines should not be understated. Just as SDG&E actively follows industry standards when implementing technical solutions, the use of such standards to "future proof" systems have been highlighted by leaders in the information technology and security industries. In its discussion on the topic of using standards as a strategy to future proof authorization, the international digital security company Gemalto[43] stated:

> Strategy #5: Leverage Standards
>
> As organizations look to ensure their authentication infrastructures have the agility needed, they'll be well served by leveraging open standards wherever possible. For example, as organizations employ cloud applications from multiple vendors, having separate authentication mechanisms means users have to login separately for each application.
>
> Security Assertion Markup Language (SAML) is an open standard for exchanging authentication and authorization data between parties. SAML not only provides a bridge between enterprise identity and SaaS applications, it also enhances the end-user experience by providing SSO capabilities across applications. OAuth (Open Authorization) is another open standard for authorization. Long term, leveraging standards like

[42] *See* Resolution, OP 23, which states, "PG&E, SCE [Southern California Edison Company], and SDG&E shall take steps to plan for future expansion of the solution(s) to other distributed energy resource and energy management providers now, in order to 'future-proof' the click-through authorization solution(s)."

[43] Gemalto is an international digital security company providing software applications, secure personal devices such as smart cards and tokens, and managed services. It is the world's largest manufacturer of subscriber identity module ("SIM") cards.

> SAML, OAuth, and the like will be become critical success factors to managing a consistent identity framework across on-premise and cloud environments.
>
> '"I would advocate decision-makers really learn about emerging standards and interfaces,'" Rothman declared. '"The reality is that, for most companies, there will be a lot of applications and services in use, which requires a lot of integration work. The more security teams understand and work with standards, the better equipped they'll be to enable new services and ensure interoperability.'[44]

NIST also highlights the importance of standards as a key to achieving portability of solutions and keeping future migration costs low:

> Standards are key to achieving portability. Building on existing standards and specifications that are known to work and are in widespread use and documenting how the standards are implemented, allows developers to continue to use their chosen development languages and tools as they build for cloud systems. This keeps migration costs and risks low by enabling organizations to leverage their IT staff's current skills, and by providing a secure migration path that preserves existing investments.[45]

The Alternate Solution proposal follows neither the OAuth nor the MFA standards, and as proposed, would result in building a custom, non-standards-based, and inherently unsecure, platform. In contrast to the Alternate Solution proposal, the architecture and implementation of the current CTP is: (1) known to function securely; and (2) properly follows the OAuth standard pursuant to IETF's documented specifications and recommendations for that framework. As such, the existing CTP is the only "standard" solution that SDG&E should be implementing as future enhancements and expansions of the platform are considered by the Commission.

[44] *See* SafeNet, *Future-Proofing Your Authentication Infrastructure, Key Strategies for Maximizing Security and Flexibility in the Long Term White Paper* (2011) at 5, *available at* https://www2.gemalto.com/adwords/authentication/whitepaper/assets/FutureProofingYourAuthenticationInfrastructure_WP_(EN)_web.pdf.

[45] *See* NIST, *NIST Cloud* Computing *Standards Roadmap* (July 2013) at 43, *available at* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf.

E. Technical Risks Related to the Authentication and Authorization Gaps Presented by the Alternate Solution

The following section discusses the technical risks of the Alternate Solution proposal resulting from a solution where the OAuth standard is not properly followed. As discussed above, the Alternate Solution proposes that customer authentication and authorization processes would be established and implemented by the third-party DRP. SDG&E would release customer data to the DRP after the DRP notifies SDG&E that its customer has authorized such release. Without independent verification (the precise outcome that the Alternate Solution seeks to achieve), the customer's data is exposed to unauthorized release to a third-party or use for unauthorized purposes. The implications of this scenario (the misuse or misappropriation of customer authorization) have been outlined by IETF in an RFC entitled" OAuth 2.0 Threat Model and Security Considerations":

> When a client requests access to protected resources, the authorization flow normally involves the resource owner's explicit response to the access request, either granting or denying access to the protected resources. A malicious client can exploit knowledge of the structure of this flow in order to gain authorization without the resource owner's consent, by transmitting the necessary requests programmatically and simulating the flow against the authorization server. That way, the client may gain access to the victim's resources without her approval. An authorization server will be vulnerable to this threat if it uses non-interactive authentication mechanisms or splits the authorization flow across multiple pages.[46]

Two specific risks that result from resource owner (customer) impersonation are directly applicable to the Alternate Solution as proposed. Specifically:

[46] *See* Internet Engineering Task Force, *OAuth 2.0 Threat Model and Security Considerations* (January 2013) at 32, *available at* https://tools.ietf.org/html/rfc6819#section-4.4.1.10.

> The malicious client could also request authorization for an initial scope acceptable to the user and then silently abuse the resulting session in his browser instance to '"silently"' request another scope.[47]

* * *

> Alternatively, the attacker might exploit an authorization server's ability to authenticate the resource owner automatically and without user interactions, e.g., based on certificates.[48]

In summary, with the Alternate Solution, once the authorization is obtained from the resource owner (customer), the DRP can control and modify the data sharing scope to suit its own needs before sending it to the utility. The risks posed by this proposal to both the customer and SDG&E further reinforce why the Alternate Solution should be rejected by the Commission.

F. Summary

Under any iteration, Solution 1 fails to meet industry standards, placing both the customer and SDG&E at risk. Neither Solution 1 proposal possesses standardization with MFA for authentication or standardization with OAuth for authorization. Most importantly, not only is there no consensus of the parties on a Solution 1, but both Solution 1 proposals contradict the Commission's intention to create a click through process that meets an industry standard so that it may safely and securely be used today and expanded for future use by customers and third parties. As the Commission concluded in the Resolution:

> The Utilities shall adhere to the OAuth 2.0 standard or subsequent standard agreed upon by the Customer Data Access Committee. This will provide all parties with a standard approach which will allow third-party Demand Response Providers to more efficiently utilize the click-through authorization process. If further clarification is needed, stakeholders should raise this issue in the CDAC.[49]

[47] *Id*. at 33.

[48] *Id*.

[49] *See* Resolution, at 36.

* * *

> The OAuth 2.0 standard or subsequent standard agreed upon by the Customer Data Access Committee will provide all parties with a uniform approach which will allow third-party Demand Response Providers to more efficiently utilize the click-through authorization process.[50]
>
> * * *
>
> The Utilities shall adhere to the OAuth 2.0 standard or subsequent standard agreed upon by the Customer Data Access Committee in the implementation of OAuth Solution 3.[51]

Both versions of Solution 1 fail to meet the requirements and intent of the Commission's decision. Accordingly, SDG&E recommends that the Commission reject adoption and implementation of Solution 1.

G. Cost Estimates

For the reasons described above, SDG&E opposes all versions of Solution 1 as they pose a fundamental security risk to both SDG&E and its customers. As required by the Resolution, SDG&E is submitting estimated budgets and costs for the elements contained in OP 29.[52] Should the Commission require SDG&E to implement the Alternate Solution, the capital cost estimate for that platform is $561,099 for labor with an additional $3,003,107 in non-labor as part of a sixteen-month project. The estimated costs include all phases of that project such as requirements elicitation, design, build, test and implementation. Non-labor costs represent the use of vendor professional services to build and implement the Alternate Solution. Labor costs represent the use of internal SDG&E resources to provide technical consultation, project

[50] *Id.*, Finding of Fact 28 at 91.

[51] *Id.*, OP 4 at 99.

[52] Per the Assigned Commissioner's First Amended Scoping Memo and Ruling (October 23, 2020), SDG&E will not be including a proposal and budget for bullet one of OP 29 concerning the expansion of CTP to third party DERPS and other energy management service providers.

management and business systems analysis services to the vendor during requirements, design, build, test and implementation phases of the project.

The cost estimates to operationally maintain, support and offer the Alternate Solution over a period of one year and eight months are $0 in labor with an additional $979,208 (O&M) in non-labor.[53] Examples of these costs include: (1) supporting DRP security audits; (2) supporting integration testing for DRPs to integrate to the Alternate Solution; (3) investigation and triage of reported issues or defects across any key systems supporting the Alternate Solution; and (4) refactoring and testing of code as appropriate due to ongoing changes and upgrades in downstream enterprise systems. Should the Solution 1 proposal change in any respect, the estimated costs may differ and require an update.

Due to its position that Solution 1 should not be implemented, SDG&E is not requesting any budget to implement the Alternate Solution. No funds are included in the total budget request for this work, nor are they included in the revenue requirement discussion in the Khong Testimony (Chapter 5). Although SDG&E does not recommend the implementation of the Alternate Solution, should the Commission order SDG&E to implement another version of a click-through process that takes place entirely on a third party's website, SDG&E would need to update its total estimated budget requests, and its revenue requirement.

This concludes my prepared direct testimony.

[53] Additional capital costs and ongoing O&M would be included in SDG&E's next General Rate Case.

IX. STATEMENT OF QUALIFICATIONS

My name is Tom Moses and I am an Enterprise Architect at San Diego Gas & Electric Company. My business address is 8690 Balboa Avenue, San Diego, CA 92123. My current responsibilities include defining and governing the technical and business architectures of systems that support San Diego Gas & Electric, including Customer Assistance, Customer Experience, Energy Efficiency programs, Demand Response programs, and SDG&E's Electric Rule 32. I have been employed within the Sempra Energy family of companies for 34 years, including SDG&E for the last 22 years.

I obtained my Bachelor of Science Degree in Business Administration with an emphasis in Information Systems from San Diego State University in May 1982. I obtained my Masters of Business Administration from Pepperdine University in June of 1986.

I have not previously testified before the Commission.

LIST OF ACRONYMS

API	Application Programming Interface
ATM	Automatic Teller Machine
CAISO	California Independent System Operator
CDAC	Customer Data Access Committee
CTP	Click-Through Authorization Process
DRP	Demand Response Provider
IAB	Internet Architecture Board
IETF	Internet Engineering Task Force
IOU	Investor-Owned Utilities
IRTF	Internet Research Task Force
IT	Information Technology
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OAuth	Open Authorization
OP	Ordering Paragraphs
OWASP	Open Web Application Security Project
PIN	Personal Identification Number
RFC	Request for Comment
SCE	Southern California Edison Company
SDG&E	San Diego Gas & Electric Company
W3C	World Wide Web Consortium