



Mr. Patrick Pearsall  
Duggins, Wren, Mann & Romero, LLP

July 7, 2022

RE: PO# 4400100157

Dear Patrick:

Attached is the prior month's invoice for Alliance Consulting Group's work in the Entergy Texas 2021 Depreciation Study.

It is a pleasure to work with you on this project. If you have any questions related to this invoice, please call me at (214) 473-6771.

Sincerely,

A handwritten signature in cursive script that reads "Dane Watson".

Dane Watson



101 E. Park Blvd, Suite 220  
Plano, TX 75074

# Invoice

Date	Invoice #
06/30/2022	22-0612

**Bill To:**

Patrick Pearsall  
Duggins Wren Mann & Romero, LLP  
[Ppearsall@dwmrlaw.com](mailto:Ppearsall@dwmrlaw.com)

Billing Period 6-1-22 through 6-30-22

PO#	Terms	ETI2022		
	Net 30 Days	Entergy Texas 2021 Depreciation Study		
Hours	Description	Rate	Amount	
9.25	Dane Watson	\$ 295	\$	2,728.75
3.00	Karen Ponder	\$ 195		585.00
11.00	Rebecca Richards	\$ 195		2,145.00
3.25	Teresa Stewart	\$ 80		260.00
				-
				-
	Subtotal			5,718.75
		<b>Total</b>	<b>\$</b>	<b>5,718.75</b>

**ALLIANCE CONSULTING GROUP**  
**Professional Services**  
**Jun-22**  
**Dane Watson**  
  
**Entergy TX**

<u>Date</u>	<u>Time: Hours</u>	<u>Activity</u>
01-Jun	2.00	Testimony review with atty, review additional edits & coordination call with Company
02-Jun		
03-Jun		
04-Jun		
05-Jun		
06-Jun		
07-Jun		
08-Jun	1.25	Case status call
09-Jun	0.50	Affidavit
10-Jun		
11-Jun		
12-Jun		
13-Jun		
14-Jun		
15-Jun	3.50	Status call & final review of reports & work papers; call on presentation of retirement dates
16-Jun		
17-Jun		
18-Jun		
19-Jun		
20-Jun		
21-Jun		
22-Jun	1.00	Status call
23-Jun		
24-Jun		
25-Jun		
26-Jun		
27-Jun		
28-Jun		
29-Jun	0.50	Status call
30-Jun	0.50	Call with Company
01-Jul		
Total	<u>9.25</u>	

**ALLIANCE CONSULTING GROUP**

**Professional Services**

**Jun-22**

**Karen Ponder**

**Entergy TX**

<u>Date</u>	<u>Time:</u> <u>Hours</u>	<u>Activity</u>
01-Jun		
02-Jun		
03-Jun		
04-Jun		
05-Jun		
06-Jun		
07-Jun		
08-Jun		
09-Jun		
10-Jun	1.00	Work paper review
11-Jun		
12-Jun		
13-Jun	1.00	Work papers
14-Jun		
15-Jun		
16-Jun		
17-Jun		
18-Jun		
19-Jun		
20-Jun		
21-Jun	0.50	Work papers
22-Jun	0.50	Work papers
23-Jun		
24-Jun		
25-Jun		
26-Jun		
27-Jun		
28-Jun		
29-Jun		
30-Jun		
Total	<u>3.00</u>	

**ALLIANCE CONSULTING GROUP**  
**Professional Services**  
**Jun-22**  
**Rebecca Richards**

**Entergy TX**

<u>Date</u>	<u>Time:</u> <u>Hours</u>	<u>Activity</u>
01-Jun	1.00	Testimony call with Client
02-Jun		
03-Jun	1.00	Call with Client
04-Jun		
05-Jun		
06-Jun		
07-Jun		
08-Jun		
09-Jun		
10-Jun		
11-Jun		
12-Jun		
13-Jun		
14-Jun	4.00	Revise PDF Report--HSPM revisions
15-Jun	5.00	Revise PDF Report--HSPM revisions
16-Jun		
17-Jun		
18-Jun		
19-Jun		
20-Jun		
21-Jun		
22-Jun		
23-Jun		
24-Jun		
25-Jun		
26-Jun		
27-Jun		
28-Jun		
29-Jun		
30-Jun		
Total	<u>11.00</u>	

**ALLIANCE CONSULTING GROUP**  
**Professional Services**  
**Jun-22**  
**Teresa Stewart**  
  
**Entergy TX**

<u>Date</u>	<u>Time:</u> <u>Hours</u>	<u>Activity</u>
01-Jun		
02-Jun		
03-Jun		
04-Jun		
05-Jun		
06-Jun		
07-Jun	2.00	Format report
08-Jun	1.00	Save report and appendices to PDF
09-Jun	0.25	Save updated Purpose to PDF and into Public & Confidential reports
10-Jun		
11-Jun		
12-Jun		
13-Jun		
14-Jun		
15-Jun		
16-Jun		
17-Jun		
18-Jun		
19-Jun		
20-Jun		
21-Jun		
22-Jun		
23-Jun		
24-Jun		
25-Jun		
26-Jun		
27-Jun		
28-Jun		
29-Jun		
30-Jun		
01-Jul		
Total	<u>3.25</u>	

**FIRM EXPENSE/PERSONAL REIMBURSEMENT REQUEST**

Return Check to: Denise Mitchell Date: 4/5/22

Issue Check to: Expergy

For Amount of: \$23,555.00

Case Name: 2022 ETI Rate Case Client #: 519 Matter #: 471

Date of Expense: 4/5/22

Purpose of Expense: \_\_\_\_\_

Professional Consulting services for March 2022

**ITEMIZATION OF EXPENSES**

Airfare - \$ \_\_\_\_\_ Hotel - \$ \_\_\_\_\_

Meals - \$ \_\_\_\_\_ Mileage - \$ \_\_\_\_\_

Cab Fare - \$ \_\_\_\_\_ Parking - \$ \_\_\_\_\_

Car Rental - \$ \_\_\_\_\_ Other - \$ 23,555.00

(Explain Other) Consulting services

NAME: Jay Breedveld Initials JJB

Signature:  Timekeeper # \_\_\_\_\_

Department: ER

**COPIES OF RECEIPTS MUST BE ATTACHED!!**

**For Accounting Use Only**

Chart of Account#: \_\_\_\_\_

Disbursement Code: \_\_\_\_\_

**Clear Form**

# Invoice

**EXPERGY®**

**PO Box 131185  
Dallas, TX 75313  
214 432-2500  
Tax ID# 26-3106033**

Date	Invoice #
4/4/2022	ETI-2211

Bill To:

Duggins Wren Mann & Romero,  
A Limited Liability Partnership  
Attn: Jay Breedveld  
P.O. Box 1149  
Austin, Texas 78767-1148

Billing Period: 3/1/2022 - 3/31/2022

	Terms	Project	
	Due on Receipt	ETI - Lead-Lag Study for PUCT Rate Case	
Hours	Description	Rate	Amount
73.5	Jay Joyce (President)	\$ 290	\$ 21,315
28.0	Diego Garcia (Consultant)	80	2,240
	<u>Travel Expenses</u>		
	Transportation		\$ -
	Meals		-
	Lodging		-
	Other		-
	Total Expenses		\$ -
		<b>Total</b>	<b>\$ 23,555</b>



**Expergy®**  
**Professional Services**  
**March 2022**  
**Jay Joyce**

**Entergy Texas, Inc.**  
**Lead-Lag Study for PUCT Rate Filing**

<u>Date</u>	<u>Time: Hours</u>	<u>Activity</u>
1-Mar	3.0	Work on CWC model
2-Mar	6.0	All group conf call; setting up invoice samples for staff analysis; preparing follow-up requests
9-Mar	3.0	Finalizing and sending follow-up requests; work on CWC model
11-Mar	5.0	Work on CWC model
14-Mar	4.0	Building CWC model
15-Mar	2.0	Building CWC model
16-Mar	6.5	Building CWC model
17-Mar	6.0	Work on CWC model
18-Mar	5.0	Work on CWC model
19-Mar	2.0	Work on CWC model
27-Mar	7.0	Work on CWC model
28-Mar	5.0	Work on CWC model
29-Mar	8.5	Work on CWC model
30-Mar	6.0	All group conf call; finalizing CWC calcs
31-Mar	4.5	Checking CWC calcs and links; sending CWC results to Company
TOTAL	<u>73.5</u>	

**Expergy®**  
**Professional Services**  
**March 2022**  
**Diego Garcia - Consultant**  
  
**Entergy Texas, Inc.**  
**Lead-Lag Study for PUCT Rate Filing**

<u>Date</u>	<u>Time: Hours</u>	<u>Activity</u>
5-Mar	2.0	Analysis of invoice samples; entering data into spreadsheets
7-Mar	1.0	Analysis of invoice samples; entering data into spreadsheets
8-Mar	2.0	Analysis of invoice samples; entering data into spreadsheets
9-Mar	1.0	Analysis of invoice samples; entering data into spreadsheets
14-Mar	4.0	Analysis of invoice samples; entering data into spreadsheets
15-Mar	2.0	Analysis of invoice samples; entering data into spreadsheets
20-Mar	4.0	Analysis of invoice samples; entering data into spreadsheets
21-Mar	3.0	Analysis of invoice samples; entering data into spreadsheets
22-Mar	3.0	Analysis of invoice samples; entering data into spreadsheets
23-Mar	3.0	Analysis of invoice samples; entering data into spreadsheets
27-Mar	3.0	Analysis of invoice samples; entering data into spreadsheets
TOTAL	<u>28.0</u>	

# Invoice

**EXPERGY®**

**PO Box 131185  
Dallas, TX 75313  
214 432-2500  
Tax ID# 26-3106033**

Date	Invoice #
5/2/2022	ETI-2216

Bill To:
Duggins Wren Mann & Romero, A Limited Liability Partnership Attn: Jay Breedveld P.O. Box 1149 Austin, Texas 78767-1148

Billing Period:	4/1/2022 - 4/30/2022
-----------------	----------------------

	Terms	Project	
	Due on Receipt	ETI - Lead-Lag Study for PUCT Rate Case	
Hours	Description	Rate	Amount
12.5	Jay Joyce (President)	\$ 290	\$ 3,625
0.0	Diego Garcia (Consultant)	80	-
	<u>Travel Expenses</u>		
	Transportation		\$ -
	Meals		-
	Lodging		-
	Other		-
	Total Expenses		\$ -
		<b>Total</b>	<b>\$ 3,625</b>

**Expergy®**  
**Professional Services**  
**April 2022**  
**Jay Joyce**

**Entergy Texas, Inc.**  
**Lead-Lag Study for PUCT Rate Filing**

<u>Date</u>	<u>Time:</u> <u>Hours</u>	<u>Activity</u>
21-Apr	1.0	Testimony draft
22-Apr	3.0	Testimony draft
25-Apr	3.5	Formatting and checking work papers
26-Apr	4.5	Finalizing and submitting draft testimony
29-Apr	0.5	Discuss draft testimony with S. Green
TOTAL	<u>12.5</u>	

# Invoice

**EXPERGY®**

**PO Box 131185  
Dallas, TX 75313  
214 432-2500  
Tax ID# 26-3106033**

Date	Invoice #
7/11/2022	ETI-2226

Bill To:
Duggins Wren Mann & Romero, A Limited Liability Partnership Attn: Jay Breedveld P.O. Box 1149 Austin, Texas 78767-1148

Billing Period: 5/1/2022 - 6/30/2022			
	Terms	Project	
	Due on Receipt	ETI - Lead-Lag Study for PUCT Rate Case	
Hours	Description	Rate	Amount
14.5	Jay Joyce (President)	\$ 290	\$ 4,205
0.0	Diego Garcia (Consultant)	80	-
	<u>Travel Expenses</u>		
	Transportation		\$ -
	Meals		-
	Lodging		-
	Other		-
	Total Expenses		\$ -
		<b>Total</b>	<b>\$ 4,205</b>

**Expergy®**  
**Professional Services**  
**May & June 2022**  
**Jay Joyce**

**Entergy Texas, Inc.**  
**Lead-Lag Study for PUCT Rate Filing**

<u>Date</u>	<u>Time:</u> <u>Hours</u>	<u>Activity</u>
3-May	2.0	Checking and formatting work papers
3-Jun	3.0	Checking and formatting work papers
7-Jun	5.0	Working on draft exhibits; finalizing work papers; uploading work papers to share folder
8-Jun	1.0	Weekly rate case conference call
10-Jun	3.5	Finalizing testimony, exhibits, and affidavit for submission to attys
TOTAL	<u>14.5</u>	



**Remit by mail to:**  
P. O. Box 130989  
Dallas, TX 75313-0989

**Remit by wire or ACH to:**  
Bank of America, N.A. Acct # 0180472852  
Wire Routing # 026009593  
ACH Routing # 111000025  
Int'l use only: Swift Code: BOFAUS3N

**Federal Tax ID: 75-0764921**

**Payment due upon receipt. Please  
include Invoice No. with remittance.**

Ref No.: 161330-00001-MEG3  
(512)236-2383/jyanez@jw.com

Page 1

Invoice No: 1839822  
Invoice Date: 05/13/2022

Entergy Texas, Inc.  
Attention: Cathy Garza  
cathygarza@eversheds-sutherland.com  
cc: sarahmerrick@eversheds-sutherland.com  
christinathompson@eversheds-sutherland.com  
Austin, TX 78701

**Re: Rate Case Expense Expert**

**FOR LEGAL SERVICES RENDERED** and expenses incurred in connection with the above-referenced matter for the period ending April 30, 2022:

### INVOICE SUMMARY

Total Fees	\$2,250.00
Total Expenses	0.00
<b>Total Due This Invoice:</b>	<b>\$2,250.00</b>

UNPAID INVOICES AS OF 05/13/2022

<u>INVOICE DATE</u>	<u>INVOICE NUMBER</u>	<u>UNPAID AMOUNT</u>
04/12/2022	1833828	257.50

**TOTAL UNPAID INVOICES:** **257.50**

**TOTAL DUE:** **\$2,507.50**

Reference No.:

Invoice No: 1839822

161330-00001-MEG3

Page 2

Invoice Date: 05/13/22

**TIME DETAIL:**

<u>Date</u>	<u>Timekeeper</u>	<u>Hours</u>	<u>Description</u>
04/04/22	M. Griffiths	0.5	Call with C. Garza.
04/08/22	M. Griffiths	1.5	Prepare for and call with G. Hoyt, R. Lain and C. Garza regarding rate case expense testimony.
04/27/22	M. Griffiths	0.5	Attention to invoice and consulting agreement review for Entergy rate case expense testimony.
04/27/22	D. Willis	1.2	Compile rate case expense documents from sharefile site; print and organize for M. Griffiths review.
04/29/22	D. Willis	0.3	Review dataroom and compile recent uploaded documents.
Total Hours		4.0	

Total Fees

\$2,250.00

**TOTAL DUE THIS INVOICE:****\$2,250.00**





Remit by mail to:  
P. O. Box 130989  
Dallas, TX 75313-0989

Remit by wire or ACH to:  
Bank of America, N.A. Acct # 0180472852  
Wire Routing # 026009593  
ACH Routing # 111000025  
Int'l use only: Swift Code: BOFAUS3N

Federal Tax ID: 75-0764921

Payment due upon receipt. Please  
include Invoice No. with remittance.

Ref No.: 161330-00001-MEG3  
(512)236-2383/jyanez@jw.com

Page 1

Invoice No: 1846535  
Invoice Date: 06/22/2022

Entergy Texas, Inc.  
Attention: Cathy Garza  
cathygarza@eversheds-sutherland.com  
cc: sarahmerrick@eversheds-sutherland.com  
christinathompson@eversheds-sutherland.com  
Austin, TX 78701

Re: Rate Case Expense Expert

FOR LEGAL SERVICES RENDERED and expenses incurred in connection with the above-referenced matter for the period ending May 31, 2022:

### INVOICE SUMMARY

Total Fees	\$16,836.00
Total Expenses	0.00
<b>Total Due This Invoice:</b>	<b>\$16,836.00</b>

UNPAID INVOICES AS OF 06/22/2022

<u>INVOICE DATE</u>	<u>INVOICE NUMBER</u>	<u>UNPAID AMOUNT</u>
05/13/2022	1839822	2,250.00

**TOTAL UNPAID INVOICES:** **2,250.00**

**TOTAL DUE:** **\$19,086.00**

Reference No.:

Invoice No: 1846535

161330-00001-MEG3

Page 2

Invoice Date: 06/22/22

**TIME DETAIL:**

<u>Date</u>	<u>Timekeeper</u>	<u>Hours</u>	<u>Description</u>
05/03/22	D. Willis	0.2	Compile additional documents from Eversheds Sutherland.
05/04/22	M. Griffiths	1.2	Attention to markup and edits to rate case expense testimony and review of invoices.
05/04/22	A. Adams	0.3	Meeting with M. Griffiths to discuss rate case expense testimony and next required steps.
05/04/22	D. Willis	0.4	Compile additional documents from Eversheds Sutherland.
05/05/22	M. Griffiths	0.2	Attention to review of documents for rate case expense testimony.
05/05/22	A. Adams	6.9	Review engagement letters, invoices, prior testimony, and prior rate case expense dockets related to Entergy and revise pre-filed testimony of M. Griffiths to incorporate information regarding three legal services and nine consultants; send related correspondence to M. Griffiths.
05/06/22	M. Griffiths	1.6	Review and comment on edits to rate case expense testimony and email to C. Garza of draft testimony.
05/10/22	D. Willis	0.3	Compile recently supplied documents; update M. Griffiths' folders for her review
05/12/22	M. Griffiths	0.3	Call with C. Garza.
05/12/22	D. Willis	0.3	Review and compile recent uploaded documents to dataroom; update M. Griffiths' working folder.
05/13/22	D. Willis	0.2	Review dataroom and compile recently uploaded documents; update M. Griffiths working folder.
05/16/22	M. Griffiths	2.6	Review and comment on draft rate case expense testimony and call with C. Garza regarding same.
05/16/22	D. Willis	0.3	Review and compile new documents on sharefile site; update M. Griffiths file.
05/17/22	D. Willis	0.2	Compile recent uploaded documents to dataroom.
05/19/22	D. Willis	0.8	Review and compile documents uploaded to Eversheds' sharefile site; office conference with M. Griffiths regarding same.
05/20/22	M. Griffiths	4.6	Review and analyze invoices received through March 2022 and edit draft testimony.
05/22/22	M. Griffiths	1.2	Further edits to draft testimony and preparation for meeting with C. Garza on 5/23.
05/23/22	M. Griffiths	1.4	Meeting with C. Garza and additional review and comments on rate case expense testimony.
05/24/22	D. Willis	0.3	Assist M. Griffiths with updated filings on sharefile site.

Reference No.:

Invoice No: 1846535

161330-00001-MEG3

Page 3

Invoice Date: 06/22/22

<u>Date</u>	<u>Timekeeper</u>	<u>Hours</u>	<u>Description</u>
05/25/22	M. Griffiths	2.5	Edit and draft testimony; review and analysis of Texas case law re: recovery of attorney fees; review and analysis of testimony and final order in PUC D. 48439.
05/25/22	D. Willis	0.2	Review and compile recent uploads to Sharefile site.
Total Hours		26.0	

Total Fees

\$16,836.00

## SUMMARY BY TIMEKEEPER

	<u>Hours</u>	<u>Standard Rate</u>	<u>Discounted Rate</u>	<u>Fees</u>
<b>Partner</b>				
M. Griffiths	15.60	895.00	720.00	\$ 11,232.00
Total Partner	15.60			\$ 11,232.00
<b>Associate</b>				
A. Adams	7.20	645.00	645.00	\$ 4,644.00
Total Associate	7.20			\$ 4,644.00
<b>Paralegal</b>				
D. Willis	3.20	300.00	300.00	\$ 960.00
Total Paralegal	3.20			\$ 960.00
<b>TOTAL</b>	<u>26.00</u>			<u>\$ 16,836.00</u>

TOTAL DUE THIS INVOICE:

\$16,836.00

**FIRM EXPENSE/PERSONAL REIMBURSEMENT REQUEST**

Return Check to: Denise Mitchell Date: 3/21/22

Issue Check to: Lewis & Ellis

For Amount of: \$980.00

Case Name: 2022 ETI Rate Case Client #: 519 Matter #: 471

Date of Expense: 3/21/22

Purpose of Expense: \_\_\_\_\_

Professional Consulting services for February 2022

**ITEMIZATION OF EXPENSES**

Airfare - \$ \_\_\_\_\_ Hotel - \$ \_\_\_\_\_

Meals - \$ \_\_\_\_\_ Mileage - \$ \_\_\_\_\_

Cab Fare - \$ \_\_\_\_\_ Parking - \$ \_\_\_\_\_

Car Rental - \$ \_\_\_\_\_ Other - \$ 980.00

(Explain Other) Consulting services

NAME: Scott Olson Initials JJB

Signature: Scott Olson Timekeeper # \_\_\_\_\_

Department: ER

**COPIES OF RECEIPTS MUST BE ATTACHED!!**

**For Accounting Use Only**

Chart of Account#: \_\_\_\_\_

Disbursement Code: \_\_\_\_\_

**Clear Form**



**Lewis & Ellis, Inc.**

6600 Chase Oaks Blvd, Suite 150

Plano, TX 75023

Tel: (972) 850-0850 Fax: (972) 850-0851

BILLING: dwebb@lewisellis.com

Tax ID: 75-1281520

Duggins Wren Mann & Romero, LLP  
Attn: Scott Olson  
P.O. Box 1149  
Austin, TX 78767

Invoice #26367  
Acct #0373

03/09/22

**Services for February, 2022:**

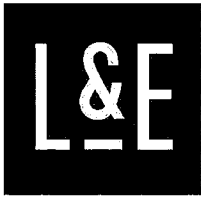
Entergy Storm Damage Reserves	\$980.00
Sub-total	\$980.00

<b>Current Amount Due</b>	<b>\$980.00</b>
<b>TOTAL AMOUNT DUE</b>	<b>\$980.00</b>

*Due immediately upon receipt*

**Actuarial Services Through February 2022**

Project	Task	Date	Employee	Hours	Bill Rate	Total
Testimony for Rate Case	Kickoff Call	1/12/2022	Gregory S Wilson	2.00	\$490	\$980.00
Net Invoice						\$980.00
<b>Direct Expenses</b>						\$0.00
<b>Current Amount Due</b>						<b>\$980.00</b>



**Lewis & Ellis, Inc.**  
6600 Chase Oaks Blvd. Suite 150  
Plano, TX 75023, United States  
Tel: 972-850-0850

Attn: Scott Olson  
Duggins Wren Mann & Romero, LLP  
P.O. Box 1149  
Austin, TX 78767

**Invoice** #26663  
**Acct** #Duggins Wren Mann  
& Romero, LLP

04/30/22

**Services for March, 2022**

Entergy Storm Damage Reserves

\$6,615.00

**Sub-Total** **\$6,615.00**

**Current Amount Due** **\$6,615.00**

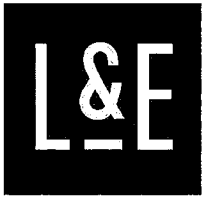
**Previous Balance** **\$0.00**

**Total Amount Due** **\$6,615.00**

*Due immediately upon receipt*







**Lewis & Ellis, Inc.**  
6600 Chase Oaks Blvd. Suite 150  
Plano, TX 75023, United States  
Tel: 972-850-0850

Attn: Scott Olson  
Duggins Wren Mann & Romero, LLP  
P.O. Box 1149  
Austin, TX 78767

**Invoice** #26929  
**Acct** #0373

05/31/22

**Services for April, 2022**

Entergy Storm Damage Reserves

\$3,430.00

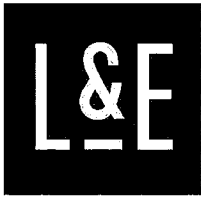
**Sub-Total** **\$3,430.00**

**Current Amount Due** **\$3,430.00**

*Due immediately upon receipt*

**Actuarial Services Through April 2022**

Project	Task	Date	Employee	Hours	Bill Rate	Total
Testimony for Rate Case	Prepare estimate	4/5/2022	Gregory S Wilson	2.50	\$490	\$1,225.00
	Prepare estimate	4/6/2022		2.00	\$490	\$980.00
	Discuss and edit estimate	4/14/2022		0.50	\$490	\$245.00
	Discuss and edit estimate	4/28/2022		1.00	\$490	\$490.00
	Discuss and edit estimate	4/29/2022		1.00	\$490	\$490.00
Net Invoice						\$3,430.00
Direct Expenses						\$0.00
Current Amount Due						\$3,430.00



**Lewis & Ellis, Inc.**  
6600 Chase Oaks Blvd. Suite 150  
Plano, TX 75023, United States  
Tel: 972-850-0850

Attn: Scott Olson  
Duggins Wren Mann & Romero, LLP  
P.O. Box 1149  
Austin, TX 78767

**Invoice** #27156  
**Acct** #0373

06/25/22

**Services for May, 2022**

Entergy Storm Damage Reserves

\$4,655.00

**Sub-Total** **\$4,655.00**

**Current Amount Due** **\$4,655.00**

*Due immediately upon receipt*

**Deloitte & Touche LLP**

701 Poydras Street, Suite 4200  
New Orleans, LA 70139-7704  
USA

Tel: +1 504 581 2727  
[www.deloitte.com](http://www.deloitte.com)

May 5, 2022

Mr. Patrick J. Condon  
Chairman  
The Audit Committee of Entergy Corporation  
726 Stonebridge Road  
Frankfort, IL 60423

Ms. Kimberly Fontan  
Senior Vice President and Chief Accounting Officer  
Entergy Texas, Inc.  
639 Loyola Avenue  
New Orleans, LA 70113

Dear Mr. Condon and Ms. Fontan:

Deloitte & Touche LLP ("D&T" or "we" or "us") is pleased to serve as independent accountants for Entergy Texas, Inc. (the "Company" or "you" or "your") to perform an examination of the management's assertion that the Summary of Costs Billed by Entergy Services, LLC and Other Entergy Affiliates to Entergy Texas, Inc. for the year ended December 31, 2021 ("Summary of Costs Billed") is in compliance with the service agreements that were previously approved by the Securities and Exchange Commission ("SEC") under PUHCA 1935 and those subsequently accepted by the Federal Energy Regulatory Commission ("FERC") following adoption of PUHCA 2005, as further described by the Notes to the Summary of Costs Billed. Ms. Amy Parker will be responsible for the services that we perform for the Company hereunder.

The services to be performed by D&T pursuant to this engagement are subject to the terms and conditions set forth herein and in the accompanying appendices. Such terms and conditions shall be effective as of the date of the commencement of such services.

**Examination of Management's Assertion**

Our engagement is to perform an examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) (the "AICPA standards"). The objective of an examination conducted in accordance with the AICPA standards is the expression of an opinion on whether the assertion is fairly stated, in all material respects, based on the criteria.

An examination includes examining, on a test basis, evidence supporting management's assertion and performing such other procedures as D&T considers necessary in the circumstances. An examination conducted in accordance with the AICPA standards is designed to obtain reasonable, rather than absolute, assurance about management's assertion taken as a whole. An examination is not designed to express an opinion on individual amounts or statements within an assertion. An examination is not designed to provide assurance on internal control or to identify deficiencies in internal control.

**D&T Reports**

We expect to issue a written report upon the completion of our examination. Our ability to express any opinion or to issue any report as a result of this engagement and the wording thereof, will, of course, be dependent on the facts and circumstances at the date of our report. If, for any reason, we are unable to complete our examination or are unable to form or have not formed any opinion, we may decline to express any opinion or decline to issue any report as a result of this engagement. If we are unable to complete our examination or if any report to be issued by D&T as a result of this engagement requires modification, the reasons for this will be discussed with the Audit Committee of Entergy Corporation (the "Audit Committee") and the Company's management.

**Management's Responsibilities**

Appendix A describes management's responsibilities.

**Responsibility of the Audit Committee**

We acknowledge that the Audit Committee is directly responsible for the appointment, compensation, and oversight of our work, and, accordingly, except as otherwise specifically noted, we will report directly to the Audit Committee. You have advised us that the services to be performed under this engagement letter, including, where applicable, the use by D&T of affiliates or related entities as subcontractors in connection with this engagement, have been approved by the Audit Committee in accordance with the Audit Committee's established preapproval policies and procedures.

**Other Communications Arising from the Examination**

In connection with our examination, we may have other comments for management on matters observed by us and possible ways to improve the efficiency of the Company's operations or other recommendations concerning internal control. With respect to these other communications, it is our practice to discuss all comments, if appropriate, with the level of management responsible for the matters, prior to their communication to senior management or the Audit Committee.

**Fees**

We estimate that our fees for this engagement will be \$150,000, plus expenses. Based on the anticipated timing of the work, our fees will be billed in May 2022 and payment is due 30 days from the date of invoice. Engagement-related expenses will be billed in addition to the fees and will be stated separately on the invoice.

Our continued service on this engagement is dependent upon payment of our invoices in accordance with these terms. Our estimated fees are based on certain assumptions, including (1) timely and accurate completion of the requested entity participation schedules and additional supporting information, (2) no inefficiencies during the examination process or changes in scope caused by events that are beyond our control, (3) the effectiveness of internal control throughout the period under examination, and (4) no changes to the timing or extent of our work plans. We will notify you promptly of any circumstances we encounter that could significantly affect our estimate and discuss with you any additional fees, as necessary.

**Restriction on Report Use**

The Company agrees that any report issued by D&T on management's assertion is intended solely for the information and use of the Company, Entergy Services, LLC, Duggins Wren Mann & Romero LLP,

Eversheds Sutherland LLP, and the Texas Public Utility Commission, and that our report is not intended to be and should not be used by anyone other than the Company, Entergy Services, LLC, Duggins Wren Mann & Romero LLP, Eversheds Sutherland LLP, and the Texas Public Utility Commission; nor will it be made available to any other persons or entities, or included, incorporated by reference, or referred to, in any filings with regulators.

\* \* \* \* \*

The parties acknowledge and agree that D&T is being engaged under this engagement letter to provide only the services described herein. Should the Company or the Audit Committee request, and should D&T agree to provide, services beyond those described herein, such services will constitute a separate engagement and will be governed by a separate engagement letter.

This engagement letter, including Appendices A through E attached hereto and made a part hereof, constitutes the entire agreement between the parties with respect to this engagement and supersedes any other prior or contemporaneous agreements or understandings between the parties, whether written or oral, relating to this engagement.

If the above terms are acceptable and the services described are in accordance with your understanding, please sign the copy of this engagement letter in the space provided and return it to us.

Yours truly,

*Dewitt Stouche LLP*

Acknowledged and approved on behalf of  
the Audit Committee of Entergy Corporation:

By: Patrick J. Condon

Title: Audit Committee Chair

Date: 06-May-2022 | 7:33:18 AM CDT

Accepted and agreed to by Entergy Texas, Inc.:

By: Kimberly A. Fontan

Title: SVP, CAO

Date: 05-May-2022 | 6:13:26 PM CDT

**APPENDIX A****MANAGEMENT'S RESPONSIBILITIES**

This Appendix A is part of the engagement letter dated May 5, 2022, between Deloitte & Touche LLP and Entergy Texas, Inc. and approved by the Audit Committee of Entergy Corporation.

**Management's Assertion**

Management is responsible for the preparation, presentation, and overall accuracy of management's assertion and its conformity with the criteria. In this regard, management has the responsibility for, among other things:

- Determining that the criteria selected are appropriate for its purposes
- Establishing and maintaining effective internal control over management's assertion
- Identifying and ensuring that the Company complies with the laws and regulations applicable to its activities and informing us of any known material violations of such laws or regulations
- Making determinations as to the relevancy of information to be included
- Making appropriate estimates and assumptions that affect reported information
- Providing us with (1) access to all information of which management is aware that is relevant to the preparation and presentation of management's assertion, such as records, documentation, and other matters, (2) additional information that we may request from management for the purpose of our examination, and (3) unrestricted access to personnel within the Company from whom we determine it necessary to obtain evidence.

**Management's Representations**

We will make specific inquiries of the Company's management about the representations embodied in management's assertion. In addition, we will request that management provide us with the written representations the Company is required to provide to its independent accountants under the AICPA standards. The responses to those inquiries and the written representations of management are part of the evidential matter that D&T will rely on in forming its opinion on management's assertion.

**Process for Obtaining Preapproval of Services**

Management is responsible for the coordination of obtaining the preapproval of the Audit Committee, in accordance with the Audit Committee's preapproval process, for any services to be provided by D&T to the Company.

**Independence Matters**

In connection with our engagement, D&T, management, and the Audit Committee will assume certain roles and responsibilities in an effort to assist D&T in maintaining independence. D&T will communicate to its partners, principals, and employees that the Company is an attest client. Management of the Company will ensure that the Company has policies and procedures in place for the purpose of ensuring that the Company will not act to engage D&T or accept from D&T any service that under the AICPA or other applicable rules would impair D&T's independence. All potential services are to be discussed with Ms. Parker.

Management will coordinate with D&T to ensure that D&T's independence is not impaired by hiring former or current D&T partners, principals, or professional employees in a key position, as defined in the AICPA *Code of Professional Conduct*, that would cause a violation of the AICPA *Code of Professional Conduct* or other applicable independence rules. Management of the Company will ensure that the Company also has policies and procedures in place for purposes of ensuring that D&T's independence will not be impaired by hiring a former or current D&T partner, principal, or professional employee in a key position that would cause a violation of the AICPA *Code of Professional Conduct* or other applicable independence rules. Any employment opportunities with the Company for a former or current D&T partner, principal, or professional employee should be discussed with Ms. Parker before entering into substantive employment conversations with the former or current D&T partner, principal, or professional employee.

For purposes of the preceding sections entitled “Independence Matters” and “Process for Obtaining Preapproval of Services”, “D&T” shall mean Deloitte & Touche LLP and its subsidiaries; Deloitte Touche Tohmatsu Limited, its member firms, the affiliates of Deloitte & Touche LLP, Deloitte Touche Tohmatsu Limited and its member firms; and, in all cases, any successor or assignee.



## APPENDIX B

## GENERAL BUSINESS TERMS

This Appendix B is part of the engagement letter to which these terms are attached (the engagement letter, including its appendices, the “engagement letter”) dated May 5, 2022, between Deloitte & Touche LLP and Entergy Texas, Inc. and approved by the Audit Committee of Entergy Corporation.

1. Limitation on Liability, Release, and Indemnification.
  - a) D&T (as defined below) and its personnel will not be liable to the Company and the Audit Committee for any claims, liabilities, or expenses relating to this engagement (“Claims”) for an aggregate amount in excess of the fees paid by the Company to D&T pursuant to this engagement, except to the extent resulting from the bad faith or intentional misconduct of D&T. In no event will D&T or its personnel be liable for consequential, special, indirect, incidental, punitive or exemplary loss, damage, or expense relating to this engagement.
  - b) The Company agrees to release and indemnify D&T and its personnel from all Claims attributable to any misrepresentation by the Company’s management.
  - c) The Company agrees to indemnify and hold harmless D&T and its personnel from all Claims, except to the extent resulting from the bad faith or intentional misconduct of D&T.
  - d) The provisions of this Paragraph 1 will apply to the fullest extent of the law, whether in contract, statute, tort (such as *negligence*), or otherwise. In circumstances where all or any portion of the provisions of this Paragraph 1 are unavailable, D&T’s aggregate liability for any Claim shall not exceed an amount that is proportional to the relative fault that D&T’s conduct bears to all other conduct giving rise to such Claim.
2. Independent Contractor. D&T is an independent contractor and D&T is not, and will not be considered to be, an agent, partner, fiduciary, or representative of the Company or the Audit Committee.
3. Survival. The agreements and undertakings of the Company and the Audit Committee contained in the engagement letter will survive the completion or termination of this engagement. For purposes of these terms, “D&T” shall mean Deloitte & Touche LLP and its subsidiaries; to the extent that, as a subcontractor, they agree to provide any of the services under or in connection with the engagement letter, the member firms of Deloitte Touche Tohmatsu Limited, and the affiliates of Deloitte & Touche LLP and such member firms; and, in all cases, any successor or assignee.
4. Assignment and Subcontracting. Except as provided below, no party may assign any of its rights or obligations (including, without limitation, interests or Claims) relating to this engagement without the prior written consent of the other parties. The Company and the Audit Committee hereby consent to D&T subcontracting a portion of its services under this engagement to any affiliate or related entity, whether located within or outside of the United States; provided, however, that such subcontracting will not relieve D&T of any of its obligations to the Company hereunder. D&T agrees that it will be responsible for the services performed by its subcontractors to the same extent that it is responsible for the services performed by itself. Professional services performed hereunder by any of D&T’s affiliates or related entities shall be invoiced as professional fees, and any related expenses shall be invoiced as expenses, unless otherwise agreed.
5. Severability. If any term of the engagement letter is unenforceable, such term shall not affect the other terms, but such unenforceable term shall be deemed modified to the extent necessary to render it enforceable, preserving to the fullest extent permissible the intent of the parties set forth herein.
6. Force Majeure. No party shall be deemed to be in breach of the engagement letter as a result of any delays or non-performance directly or indirectly resulting from circumstances or causes beyond its reasonable control, including, without limitation, fire, epidemic or other casualty, act of God, strike or labor dispute, war or other violence, or any law, order or requirement of any governmental agency or authority.
7. Protection of Personal Information. To the extent that any information obtained by D&T from or on behalf of the Company or its employees in connection with the performance of services under this engagement letter relates to a resident of Massachusetts and constitutes “Personal Information” as defined in 201 CMR 17.02 (as may be amended), D&T shall comply with the obligations of 201 CMR 17.00 et. seq. (as may be amended), entitled “Standards for the Protection of Personal Information of Residents of the Commonwealth,” with respect to such information.

- 8a. Confidentiality. All nonpublic data provided to D&T disclosed or made available to D&T or obtained by D&T, directly or indirectly, from you and is in D&T's possession in connection with the performance of services under this engagement letter shall be deemed confidential information belonging to the Company (together with Personal Information (as defined below), the "Confidential Information"). Confidential Information does not include the independent auditor's report that will be issued pursuant to this engagement letter. During the term of this engagement letter and thereafter, D&T shall not disclose such Confidential Information to third parties without your prior written consent except (i) to the extent reasonably necessary in connection with the performance of the services herein, or (ii) where such Confidential Information was publicly available, or (iii) if such Confidential Information was either actually known to D&T prior to the Company's disclosure of such information under this engagement, or became available to D&T on a nonconfidential basis from a source other than the Company that D&T reasonably believes was not prohibited from disclosing such information to D&T by obligation to the Company, or was independently obtained or developed by D&T outside of disclosures made hereunder. Notwithstanding anything to the contrary contained herein, D&T shall not be restricted from, and the Company hereby consents to D&T disclosing and providing Confidential Information (1) to contractors providing administrative, infrastructure, and other support services to D&T and subcontractors providing services in connection with this engagement, in each case, whether located within or outside of the United States, provided that such contractors and subcontractors have agreed to be bound by confidentiality obligations similar to those in this paragraph; and (2) as may be required by law or regulation, or to respond to governmental inquiries, or in accordance with applicable professional standards or rules or in connection with litigation or arbitration pertaining hereto; provided, that if such disclosures are made as required by law or court order, then D&T, to the extent reasonably practical, shall give prompt advance notice of such disclosure requirement and shall request confidential treatment for the Confidential Information ordered or required to be disclosed. In satisfying its obligations under this paragraph, D&T shall maintain the Company's trade secrets and proprietary or confidential information in confidence using at least the same degree of care as it employs in maintaining in confidence its own trade secrets and proprietary or confidential information, but in no event less than a reasonable degree of care.
- 8b. Terms.
- i. "Personal Information" means any non-public information capable of individually identifying a natural person, in written or electronic form, that is received from, or on behalf of, the Company by D&T during and pursuant to performance of the services hereunder. Personal Information does not include Protected Health Information, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009 (the "HITECH Act").
  - ii. "Privacy Laws" means applicable privacy and consumer protection rules, laws and regulations, and orders, including any state and federal to which D&T may be subject and which D&T is required by applicable law to comply with in the performance of services hereunder.
- 8c. Compliance with Privacy Laws. D&T acknowledges that the data to which it will have access pursuant to this engagement may contain Personal Information, the use of and access to which may be subject to Privacy Laws. D&T agrees to abide by such applicable Privacy Laws pertaining to Personal Information applicable to it in the performance of the services hereunder, as they are promulgated, and to maintain physical, electronic and procedural safeguards designed to allow D&T to comply therewith.
- 8d. Personal Information Incident. In the event that D&T's engagement leader becomes aware of any breach of its confidentiality obligations set forth in the section entitled "Confidentiality" above that results in unauthorized access to Personal Information of the Company in D&T's control "unauthorized access", D&T shall promptly notify the Company of such unauthorized access and reasonably cooperate with the Company in complying with any Company notification obligations required by applicable law.
- 8e. Liability in Connection with an Incident. To the extent that such unauthorized access (described in the section entitled "Personal Information Incident" above) arises out of D&T's intentional misconduct or breach of its confidentiality obligations under the section entitled "Confidentiality" above with respect to Confidential Information which is Personal Information, then, to the extent any Company notification is required by applicable law, D&T shall reimburse the Company for the reasonable out of pocket costs of notifying such affected individuals and providing such individuals with one year of credit monitoring service, in an aggregate amount not to exceed \$1,000,000.
9. Dispute Resolution. Any controversy or claim between the parties arising out of or relating to the engagement letter or this engagement (a "Dispute") shall be resolved by mediation or binding arbitration as set forth in the Dispute Resolution Provision attached hereto as Appendix C and made a part hereof.

## APPENDIX C

## DISPUTE RESOLUTION PROVISION

This Appendix C is part of the engagement letter dated May 5, 2022 between Deloitte & Touche LLP and Entergy Texas, Inc. and approved by the Audit Committee of Entergy Corporation.

This Dispute Resolution Provision sets forth the dispute resolution process and procedures applicable to the resolution of Disputes and shall apply to the fullest extent of the law, whether in contract, statute, tort (such as *negligence*), or otherwise.

Mediation: All Disputes shall be first submitted to nonbinding confidential mediation by written notice to the parties, and shall be treated as compromise and settlement negotiations under the standards set forth in the Federal Rules of Evidence and all applicable state counterparts, together with any applicable statutes protecting the confidentiality of mediations or settlement discussions. If the parties cannot agree on a mediator, the International Institute for Conflict Prevention and Resolution ("CPR"), at the written request of a party, shall designate a mediator.

Arbitration Procedures: If a Dispute has not been resolved within 90 days after the effective date of the written notice beginning the mediation process (or such longer period, if the parties so agree in writing), the mediation shall terminate and the Dispute shall be settled by binding arbitration to be held in New York, New York. The arbitration shall be solely between the parties and shall be conducted in accordance with the CPR Rules for Non-Administered Arbitration that are in effect at the time of the commencement of the arbitration, except to the extent modified by this Dispute Resolution Provision (the "Rules").

The arbitration shall be conducted before a panel of three arbitrators. Each of the Company and Deloitte & Touche LLP shall designate one arbitrator in accordance with the "screened" appointment procedure provided in the Rules and the two party-designated arbitrators shall jointly select the third in accordance with the Rules. No arbitrator may serve on the panel unless he or she has agreed in writing to enforce the terms of the engagement letter (including its appendices) to which this Dispute Resolution Provision is attached and to abide by the terms of this Dispute Resolution Provision. Except with respect to the interpretation and enforcement of these arbitration procedures (which shall be governed by the Federal Arbitration Act), the arbitrators shall apply the laws of the State of New York (without giving effect to its choice of law principles) in connection with the Dispute. The arbitrators shall have no power to award damages inconsistent with the terms of the engagement letter or its appendices, including, without limitation, the limitation on liability, release and indemnification provisions contained therein. The arbitrators may render a summary disposition relative to all or some of the issues, provided that the responding party has had an adequate opportunity to respond to any such application for such disposition. Discovery shall be conducted in accordance with the Rules.

All aspects of the arbitration shall be treated as confidential, as provided in the Rules. Before making any disclosure permitted by the Rules, a party shall give written notice to all other parties and afford such parties a reasonable opportunity to protect their interests. Further, judgment on the arbitrators' award may be entered in any court having jurisdiction.

Costs: Each party shall bear its own costs in both the mediation and the arbitration; however, the parties shall share the fees and expenses of both the mediators and the arbitrators equally.

## APPENDIX D

## INSURANCE

This Appendix D is part of the engagement letter dated May 5, 2022, between Deloitte & Touche LLP and Entergy Texas, Inc. and approved by the Audit Committee of Entergy Corporation.

1. Without limiting any obligations or liabilities of D&T under this engagement, D&T shall provide and maintain during the term of this engagement, at its own expense, without direct reimbursement, insurance coverage in forms and amounts which D&T believes will adequately protect it, but in no case less than:
  - (a) Errors and omissions liability insurance as may be appropriate and available in the amount of not less than \$1,000,000 per claim covering claims or damages because of injury or damages arising out of any act, error, or omission of D&T in the rendering of professional services; and
  - (b) Data security insurance coverage, insuring security and privacy liability as well as data breach costs (including notification expenses and event management costs) with liability limits of \$1 million per event.
2. D&T hereby waives all rights of recourse, including any right to which another may be subrogated, against you and Entergy Corporation subsidiaries ("Entergy Affiliates") for personal injury, including death, and property damage.
3. All of D&T's policies of insurance shall be primary and non-contributing with any insurance maintained by you and Entergy Affiliates. D&T will provide you with thirty (30) days' prior written notice of cancellation or any material adverse change in conditions.
4. D&T shall provide you with certificates of insurance issued to you and Entergy Affiliates as the certificate holder, evidencing coverage currently in effect upon execution and for the duration of this engagement. D&T shall require any subcontractor providing on-site services under this engagement to carry insurance coverage in a form and amount consistent with the requirements of this Appendix N. D&T shall obtain certificates of insurance evidencing such coverages prior to the commencement of services by the subcontractor, and shall present such certificates to you upon request and, in any case, no later than completion of services hereunder.
5. D&T and any subcontractor shall not begin the services until all of the insurance required of D&T and any subcontractor is in force and you have received the necessary documents. Compliance with this requirement is hereby expressly made a condition precedent to your obligation to make payment for any services performed. The minimum insurance requirements set forth above shall not vary, limit or waive D&T's or its subcontractor's legal or contractual responsibilities or liabilities to any party.

**APPENDIX E****INFORMATION SECURITY STATEMENT****Overview**

Deloitte has implemented an Information Technology (IT) infrastructure that is designed to align with industry standards. The security boundary of the IT infrastructure includes Deloitte-issued laptops, as well as infrastructure and applications, such as databases and backup systems. The IT infrastructure security controls and associated information security processes were developed to protect confidential information. In addition, Deloitte has developed and implemented resiliency processes related to protection of Deloitte people, its facilities, and continuity of operations. A summary of such processes, as well as policies and controls, are set forth below.

**Purpose**

The purpose of this Information Security Statement is to provide an overview of Deloitte's security practices that are in effect as of the published date of this document (09/02/2021).

**Information Security Program**

Deloitte maintains a comprehensive information security program, which includes policies, standards, procedures, and guidelines. The information security program is informed by several industry-standard guidelines and best practices including ISO 27001, COBIT, ITIL, and the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC 2).

Deloitte's IT leadership meets on a regular basis to consider strategic and tactical direction for the information security program, and its policies, standards, procedures, and guidelines.

Information security policies are drafted with input from internal information security stakeholders and are based upon industry-standard practices. The drafts are reviewed and approved by Deloitte's Cyber Security leadership, Office of General Counsel (OGC), Chief Confidentiality & Privacy Officer, Chief Information Officer (CIO), and Chief Information Security Officer (CISO). Once approved, the policies are published on Deloitte's Intranet and communicated to personnel at least annually.

**Security Assurance and Certifications**

Deloitte has established the following security assurance and certifications programs:

**Information Security Management System (ISO 27001)**

Deloitte has established and operates an Information Security Management System (ISMS) that manages its client confidential information. An independent third party has certified that the ISMS complies with the requirements of the International Information Security Management System Standard ISO 27001.

**Business Continuity Management System (ISO 22301)**

Deloitte's Business Continuity Management System (BCMS) program has been certified by an independent third party that it complies with the requirements of ISO 22301. This certification requires Deloitte to demonstrate the effectiveness of its BCMS program, and specifies the requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented business continuity management system to protect against, prepare for, respond to, and recover from disruptive incidents when they arise.

**Third Party Assessments**

Deloitte's Information Security program is assessed by third parties. The focus of the assessments is to measure the overall maturity and effectiveness of Deloitte's Information Security program. The comprehensive reports may be obtained by current or prospective clients with an acceptance of appropriate non-disclosure or confidentiality terms with Deloitte and subscriptions from the respective third parties.

**On-Site Security Assessments**

In an effort to protect and minimize risks to Deloitte's client data, and in lieu of permitting individual clients to perform independent security assessments of Deloitte's information security program, each year Deloitte engages an independent third-party auditor (Third Party) to conduct examinations in accordance with the Statement on Standards for Attestation Engagements to report on controls at a Service Organization (SOC 2 Report).

**SOC 2 Report**

The SOC 2 Report includes the Third Party's opinion on the fairness of the presentation of the description of Deloitte's systems in management's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on the Third Party's examination. The SOC 2 Report also includes a description of Deloitte's systems and controls, and a description of the Third Party's criteria, test procedures, and the results of such tests. The SOC 2 Report may be made available to a current or prospective client that is bound by appropriate non-disclosure or confidentiality terms with Deloitte applicable to the disclosure of the SOC 2 Report.

**Awareness and Training**

Deloitte has implemented training and awareness programs for its personnel related to information security, confidentiality, and privacy policies and practices. Deloitte personnel are required to complete information security, confidentiality, and privacy trainings during the new-hire onboarding process, as well as an annual update course thereafter. Deloitte personnel are presented with an information security policy awareness statement (which includes confidentiality and privacy policy requirements) via Deloitte's Intranet three times each year, which personnel are required to acknowledge within two weeks of the statement's release. In addition, Deloitte conducts internal simulated phishing campaigns to raise awareness and reduce risk among personnel.

Deloitte has a dedicated Security Awareness Committee. The committee is responsible for generating ideas to raise awareness of risks and to enhance the overall security culture through policy development and training. The committee meets regularly to discuss new and recurring security, confidentiality, and privacy issues, devise strategies and implementation plans, and to provide progress reports on existing projects. The committee is comprised of delegates from Deloitte's Cyber Security leadership, National Office of Security, Confidentiality & Privacy, Office of the CISO, National Quality Risk Management, Talent, and Office of General Counsel, and from Deloitte Touche Tohmatsu Limited's Global Information Security Office.

## **Cyber Security**

The ITS Cyber Security team safeguards Deloitte's people, data, and brand, and their services uphold Deloitte's client, legal, and regulatory requirements in an evolving cyber era. The Office of the Chief Information Security Officer (OCISO) develops an organization-wide strategy and conducts operational oversight of the ITS Cyber Security team. Deloitte's Chief Information Security Officer (CISO) oversees the ITS Cyber Security team, which provides support in the following areas:

- Cyber Security Operations:
  - Prevents, detects, and responds to an adversary's ability to steal, deny access to, or manipulate data, information or infrastructure
  - Assists in the development of security programs that enforce a structured defense to cyber risk by integrating threat intelligence data, analytics, and incident response capabilities
- Incident Response:
  - Responds to incidents, and the planning, coordinating, and validating of corrective actions related to cyber events
  - Protects Deloitte's brand, reputation, intellectual property, client and proprietary data/information, and Deloitte personnel with vigilance, preparation, and expertise
  - Provides and leverages Deloitte's expertise in threat management, digital forensics, communications, and operational intelligence to securely operate and defend Deloitte
- Security Architecture & Engineering:
  - Develops secure solutions aligned with Deloitte's policies and standards by engaging project teams, assessing cyber-related risks, coordinating the performance of risk-management activities, and reviewing solution designs for appropriate security controls
  - Implements solutions and provides ongoing operational support for security tools utilized by the Security Operations Center
- Cyber Strategic Initiatives include the following areas:
  - Identity and Access Management

- Implements tools, technologies, and organizational processes that provide end- users and administrators with secure, easy access to applications and collaboration platforms across Deloitte and with clients (core technologies include privileged access management, access management/single sign-on, multi-factor authentication, and identity governance and administration)
- Cyber Design Studio
- Minimizes cyber risks related to technology solutions developed, updated, or acquired by Deloitte
- Advises teams on security requirements, designing/assessing architectures, coordinating security testing, and confirming the completion of risk-management activities prior to release
- Data Protection
- Implements consistent security controls designed to protect client and Deloitte's personnel data and confidential information
- Provides data protection services that include data loss prevention, data access governance, data retention and destruction, data classification and rights management, cloud data protection, certificate lifecycle management, data encryption and key management, and firewall rules reviews
- Risk & Compliance
- Risk & Compliance is the integrated collection of departments that enables Deloitte to reliably achieve security and compliance objectives, act with integrity, and demonstrate capabilities to manage risk associated with information assets entrusted to Deloitte. Risk and Compliance is responsible for providing strategy, direction, and risk-management guidance to Deloitte specific to internal compliance as well as manage risk from external factors that may threaten Deloitte. Risk and Compliance consists of the following areas:
  - IT Policies, Standards & Exceptions
  - Security Awareness Program
  - Compliance Monitoring
  - Audits & Assessments (Internal and External)
  - Client Audits and Inquiries
  - ISO 27001 & Risk Assessments
  - SSAE 18 SOC 2 Reporting
  - Governance, Risk & Compliance Automation
  - Quality Assurance
  - Vendor Assessment
- Assurance & Certifications Programs:
  - Specializes in strategic assurance and certification, management of audits and



- assessments (including regulatory audits and remediation activities)
- Provides guidance and security requirements to teams conducting client engagements
- Acts as trusted advisors on cyber risk related inquiries from: clients, client engagement teams, regulators, and internal/external auditors

➤ eDiscovery, Forensics & Investigations:

- Provides support to various organizations within Deloitte, including Office of General Counsel, Talent, and Insider Threat
- Collects, processes, and retains data in support of all legal matters

Deloitte maintains an appropriately sized, dedicated staff to support the Cyber Security Program. Deloitte establishes Information Technology and Cyber Security staffing benchmarks using industry metrics, previous staffing baselines, and expected growth trends.

Members of the Cyber Security team hold various industry security and audit-based certifications (e.g., CISSP, CISM, CISA, CDPSE, ISSM, CRISC, CEH, CCSP, ISO 27001 Lead Auditor, HITRUST certified CSF Practitioner, and OSCP).

## **Asset Management**

Deloitte has asset management teams that hold shared responsibility for oversight and management of Deloitte IT assets and inventory throughout the asset lifecycle. Asset information is identified, inventoried, classified, and managed in centrally managed IT asset management systems, based on IT asset classes. There are tools and controls in place that manage hardware and software assets.

Deloitte has policies and procedures in place to manage licensed software and security controls to deter prohibited software from being installed and/or used on

Deloitte assets. Various centralized software and hardware inventory systems are maintained, which identify hardware and software components used within Deloitte information systems. These controls are supported by automated tools that provide configuration and inventory information on a continuous basis specific to configuration compliance, known vulnerabilities, inventory by Internet Protocol address (IP address) / device name and asset operational and connection status.

IT assets are configured to function in accordance with Deloitte's policies and standards, applicable specifications, and functionality requirements to prevent unauthorized or incorrect updates from being applied to such systems and network devices. Assets are provisioned using standardized and approved baseline configurations.

## **Access Control**

Access to Deloitte information contained on Deloitte IT systems is granted on a need-to-know basis and must be approved by the Deloitte data owner.

Deloitte has policies and procedures in place to manage user accounts and access for new hires, existing staff, transfers, and terminated personnel. Automated processes link the Human Resource (HR) system to administer user access.

Deloitte has a formal disciplinary process for personnel who have violated access policies. Violations are evaluated on a case-by-case basis and may result in disciplinary action, including termination and/or criminal charges, if warranted.

Vendor and contractor access are requested through procedures that involve Deloitte's Talent and Technology groups. Upon approval, the vendor user accounts are created in a controlled domain organizational unit giving the access necessary to perform their defined duties. Vendor and contractor access are granted on a temporary basis based on business need.

Remote access is provided via Transport Layer Security (TLS) using two-factor authentication with account activity being logged to Deloitte's logging/alerting mechanism. Depending on the level and type of access required, a Virtual Private Network (VPN) solution provides a secure virtual session or web interface with access into the needed application(s) or platform.

For all web-based applications (including VPN), Multi-Factor Authentication (MFA) has been enabled. Verification options include text message or mobile application.

Privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into role-based groups (e.g., key management, network, system administration, database administration, and web administration).

### **Identification and Authentication**

All users must authenticate to the Deloitte network using a unique user identification (ID) and a strong password prior to gaining access to the information system.

#### **Deloitte strong passwords contain the following characteristics:**

- Passwords are required to be at least ten (10) characters in length and contain at least three of the following four elements: (1) westernized Arabic numbers (e.g., 2,5,9), (2) non-alphanumeric characters (e.g., #, %, !, %, @, ?, -, \*), (3) English uppercase letters (e.g., A, B, C), and/or (4) English lowercase letters (e.g., a, b, c)
- Passwords are not permitted to contain:
  - parts of the users' username, first name, or last name
  - dictionary words with or without (i) numbers or special characters at the beginning or end, or (ii) letters, numbers, or character exchanges (e.g., Summer2017, ?Happyman, H3llofr!end?)
  - words or numbers connected with users such as family names, pet names, birthdays, addresses, or phone numbers
  - common terminology, acronyms, or names associated with the Deloitte or its clients
  - any variation of 'Deloitte' or 'Password' (e.g., Deloitte12, P@ssw0rd12, Pa\$\$w0rd!2)

- any sequencing of letters and numbers that follow the order of a keyboard (i.e., keyboard walk patterns such as 1234qwerASDF, 1qazXSW@3edc)

### **Additional Password Safeguards**

The following additional password related safeguards are enforced:

- Users are not permitted to reuse their previous twenty-four passwords
- Passwords expire every 90 days
- There is a password lockout threshold after 6 invalid logon attempts

## **System Security**

### **System and Communications Protection**

A firewall and intrusion prevention system (IPS) is employed at the point of entry and between various security zones within the Deloitte network. Access control lists are placed on firewalls controlling the inbound and outbound flow of traffic. Traffic is denied by default unless approved by the gateway protocols as configured and approved by the Deloitte security team. A demilitarized zone (DMZ) and trusted zones are used to segment traffic to areas that are protected in accordance with the accepted risk levels. Web servers located on a publicly reachable network segment are separated from the internal network by a firewall (i.e., DMZ).

### **System and Information Integrity**

Firewall, IPS, and VPN audit logs are sent to the log aggregator, which checks for abnormal activity and anomalous behavior that would trigger an information security review. Hardware and software checks are done by automated tools with identified alert levels that trigger a notification to the system administrators in case of a system flaw.

Anti-virus and malware protection are managed by enterprise policy and distributed periodically by a server located in the environment. Anti-virus is configured to scan external devices attached to the information system as well as email traffic.

The anti-virus software is configured to automatically update protection periodically and scan the files prior to access. Deloitte has implemented a local administrative privilege management tool to prevent users from disabling security controls (anti-virus, firewalls, DLP, CASB and others). An Advanced Threat Protection (ATP) service has been deployed to provide protection against common and sophisticated attacks against Deloitte-managed servers, laptops, and workstations. The ATP service performs three primary functions: monitor, prevent / protect, and report.

### **Network Access Controls**

Deloitte has implemented industry standard Network Access Controls (NAC) to prevent unauthorized devices from accessing the Deloitte network. The NAC and group policy settings enforce compliance checks and authentication of Deloitte managed devices for wired and wireless access.

## **Data Backup and Restore**

Production servers are scheduled for a daily, full, or incremental backup. Non-production server backups are scheduled for backup as needed. If a system backup is interrupted for any reason, it will resume in the same site once the issue that caused the interruption is resolved. In the normal operation of the data center, tape and/or disk-based backup restores are performed multiple times per week. These restores validate the integrity of backup data at rest on disk and tape. Physical tape media are stored in a secured facility. Damaged and end-of-life media is destroyed by a certified vendor and the vendor provides a confirmation of destruction. Tapes that contain data are sent off-site and tracked by an automated inventory tracking system. The off-site vendor stores the media in a secure, environmentally controlled storage facility. Backup data stored on tape and disk is encrypted using AES-256 standards.

## **Laptop Backup and Restore**

Deloitte laptops are backed up daily to a Software as a Service (SaaS) backup solution, using automated technology. All backup and restore activities are secured using 256-bit TLS v1.2 encryption. Backups are validated through periodic operational data recovery.

## **Information Systems Acquisition, Development and Maintenance**

### **Acquisition of System and Services**

Deloitte does not acquire IT systems or services until Cyber Security has reviewed the product or service to determine whether it meets internal guidelines with respect to security and encryption. Software installation requests are submitted for risk assessment and approval. Software is not implemented unless it is reviewed against Information Technology Services (ITS) standards. There is a Change Control Board (CCB) that discusses any changes that may affect the security posture of the environment and documents all proposed upgrades or modifications to the environment, assets, and infrastructure.

### **Application Development**

Deloitte follows secure coding best practices during the Secure System Development Lifecycle (SSDLC) for Deloitte applications. The SSDLC process includes requirements gathering, system analysis and design, application scanning, testing and acceptance. Deloitte's applications and their components are tested for compliance with generally accepted security standards. Testing includes manual, static, and dynamic code reviews; vulnerability scans are performed and must meet defined security levels prior to applications being placed in production.

### **Change Control**

Deloitte has a change management process in place for its IT systems. Proposed changes are submitted, tested, and reviewed during regularly scheduled Change Control Board meetings. Approved changes are tested, and vulnerability scans are performed prior to deployment. Deployment windows are scheduled to minimize the impact to Deloitte's operations. Back-out plans are in place should they be needed.

## **Patch Management**

Deloitte has a Patch Management program and supporting tools in place that are managed by an internal Patch Management Team (PMT). Vendor and industry-accepted alert lists are monitored for new patches. Patches are reviewed by the PMT during regularly scheduled meetings and are rated for deployment based on assessed severity levels. Emergency patch management meetings are called when needed.

## **Vulnerability Management**

Vulnerability scans and penetration tests are performed by independent, qualified, and authorized Deloitte staff or third parties using automated vulnerability and configuration verification tools. Penetration tests are performed annually on the network infrastructure's external perimeter by an independent team within Deloitte. Vulnerability scanning is performed weekly on the network infrastructure's internal and external perimeter by an independent Deloitte team.

## **Maintenance**

Deloitte ITS performs software and hardware maintenance on Deloitte's environment servers.

Performance reports are initiated through automated tools that specify certain levels of performance to trigger the generation of these reports (e.g., % of CPU processor utilization, etc.).

Third-party contractor maintenance personnel must be approved prior to receiving access to the information system servers. Third-party maintenance personnel are escorted into the facility and accompanied during the period of access. A log is maintained that documents the name, date, length of time, justification, and escort name for each maintenance individual who is granted access to the information system(s).

## **Wireless Access**

Deloitte supports an internal wireless network within the organization. A wireless-security and acceptable use policy is in place. Only Deloitte-approved access points will be connected to Deloitte's network. Wireless network segments are segregated from the Deloitte network using Virtual LANs or other appropriate technologies.

- For wireless access to Deloitte's networks, personnel are required to use Wi-Fi Protected Access (WPA2 or stronger protection) where it is available.
- For the convenience of visitors, clients, or guests, a guest wireless network providing controlled access to the Internet may be made available in Deloitte's facilities.
- Visitor devices may only connect to Deloitte's segregated visitor wireless network for internet access, which is separated from Deloitte's network.

## **Data Protection**

Deloitte personnel receive training on the proper handling of confidential information (CI) and Personally Identifiable Information (PII). Deloitte requires transmission of certain data in an encrypted format.

### **Data Loss Prevention**

Deloitte Data Loss Prevention (DLP) controls are enabled to monitor the following channels for data exfiltration: HTTP/S, FTP, SMTP (Email), Removable Media, Printer/Fax, and Cloud Storage. DLP controls are also configured to meet legal, regulatory, and risk requirements and align with Deloitte's security policies.

Deloitte practitioners are prohibited by a technical control from writing data to removable media devices (e.g., external hard drive, USB thumb drive, and removable hard drives) except where there is a business need.

Cloud Access Security Broker (CASB) service is used to provide a centralized view of service or application use across the Deloitte Network, help protect data, and perform anomalous behavior detection. In addition, Deloitte has implemented controls to prevent the upload of files to the following categories of sites: Storage, Collaboration, Social Media, and Webmail.

### **Media Protection**

Secure printing is available at multiple locations within each Deloitte office that requires the usage of a Deloitte-issued electronic smartcard badge to enable the print job. In addition, software has been deployed to Deloitte-issued IT assets as part of the standard application toolset that allows the creation of encrypted WinZip files (FIPS 140-2 compliant).

Laptops are encrypted and required to be physically secured at all times. Physical access to servers is restricted to authorized parties. Magnetic drives are wiped/over-written with a minimum of three passes with a media sanitization tool prior to being released for re-use and disposal.

Deloitte has employed the following methods of mobile device protection: (i) forced access Personal Identification Numbers (PINs); (ii) remote wipe after incorrect PIN/password attempt policy is exceeded; (iii) remote wipe if the mobile device is reported as lost or stolen; (iv) encryption; and (v) an installed Mobile Device Management and Mobile Threat Management tools.

### **Data Destruction**

Policies and practices are in place with regards to the destruction of confidential information and Personally Identifiable Information (PII) that vary depending on type of media on which such information is stored. Deloitte is aligned with the National Institute for Standards and Technology's (NIST) guidelines for media sanitization. Storage media is required to be wiped using a disk cleaning tool, and tapes are required to be destroyed at end-of-life. Paper containing such information is required to be discarded into secure lockboxes and is shredded by a reputable and certified third party that uses processes that meet NIST destruction standards.

## **Encryption**

Deloitte uses an industry standard Public Key Infrastructure (PKI) key management solution to manage and secure the private keys. PKI keys are generated by custodians within Deloitte. Deloitte maintains inventory of cryptographic items used in the services they provide that details all cryptographic keys, digital certificates, cryptography software, and cryptographic hardware managed by Deloitte to prevent damage in case of an incident. PKI keys are rotated annually and replaced before their expiration. Deloitte maintains a backup of all PKI keys to prevent the service being interrupted if the keys become corrupted or require restoration. Access to the backups is restricted to secure locations and access controls are based on least privileges.

Data-at-rest encryption has been employed on all block storage arrays supporting physical and virtual servers.

Whole-disk encryption has been deployed on Deloitte-issued laptops. Deloitte's laptops have deployed encryption with the 256-bit Advanced Encryption Standard (AES) algorithm.

WinZip is installed on all Deloitte-issued laptops. This encryption method is FIPS 140-2 compliant.

Deloitte Internet email gateways are configured to attempt to transmit all email in an encrypted manner, using opportunistic TLS encryption, if the recipient of the transmission can support such encryption methodology. If TLS is enabled on the recipient email gateway, the email will be encrypted between the Deloitte gateway and the recipient gateway. TLS encryption can also be enforced when agreed with the recipient organization. This encryption method is FIPS 140-2 compliant.

Data-in-transit is protected by secure TLS using certificates with minimum 2048-bit RSA key and SHA2 signing when using Deloitte secure websites and file transfer services.

Secure File Transfer Protocol (SFTP) is an available option for the transfer of client data. SFTP securely encrypts and compresses files during transmission. This encryption method is FIPS 140-2 compliant.

## **Compliance**

### **System Audit and Accountability**

System audit logs and records are created to monitor the following:

- Anti-virus services
- Intrusion prevention services
- Remote access services, web proxy services
- Domain authentication
- Router events
- Firewall events
- VPN access
- Application logs
- Operating system logs
- Privileged access logs

System audit logs are maintained to support analyses and investigations. Logs are maintained for a period of one (1) year. Logs may also be preserved for longer periods based on legal or regulatory requirements.

System audit log content includes: (i) date and time of the security event; (ii) the component of the information system (e.g., software component, hardware component) where the security event occurred; type of security event; (iv) unique user/subject identity; and (v) the outcome (success or failure) of the security event.

Deloitte's 24X7 Security Operation Center uses an industry standard Security Information and Event Management (SIEM) platform and log monitoring tools to continuously identify, prevent, and respond to operational problems, security incidents, policy violations, and fraudulent activities. System audit logs are aggregated, and security events are analyzed with appropriate correlation rules to generate alerts and respond accordingly.

### **System Audits**

Deloitte's internal audit team periodically performs internal audits on various aspects of Deloitte's systems, processes, and policies.

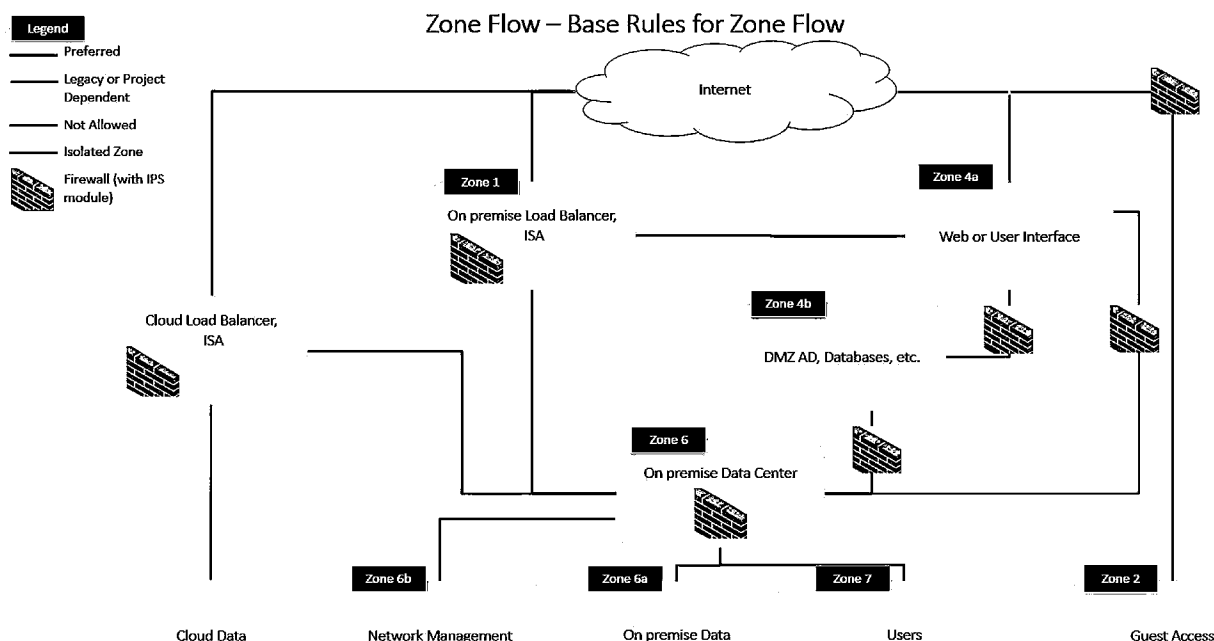
### **Application Configuration Management**

Software baseline requirements are created in accordance with Deloitte's policies and standards. Software is tested against the baseline requirements prior to being placed in the production environment. Continued monitoring and change management processes are conducted while in operation.



## Data Flow Diagram

### Zone Flow – Basic Rules for Zone Flow



### **Deloitte.**

Name: Network Diagram.pptx Revised 12/15/2020 Reviewed: 8/12/2021

## Management and Protection of Confidential Information

Deloitte is committed to protecting the Confidential Information (CI), including Personally Identifiable Information (PII), of our clients, our organization and the third parties with whom we work. “Confidential Information” refers to any information not generally available to the public, in any form, that Deloitte receives or creates in the ordinary course of business. To support this commitment, Deloitte’s Confidentiality & Privacy team is responsible for setting guidelines, developing procedures, and providing consultation and training on the management of Confidential Information.

Confidentiality & Privacy has also developed the Confidential Information Program (CIP) for the proactive management of the protection of Confidential Information and is responsible for implementing the Confidential Information Program across Deloitte. The Confidential Information Program consists of processes, technology controls, training, and communications that help our professionals to improve their awareness of risks associated with Confidential Information and their ability to properly manage and safeguard Confidential Information.

## **Confidentiality Program**

The Confidentiality Program consists of processes and activities that are performed throughout the engagement and data lifecycle to manage and protect Confidential Information.

Client account and engagement teams in the Confidentiality Program generally do the following:

- Appoint a Confidentiality & Privacy Manager responsible for overseeing program activities.
- Develop and maintain a Confidential Information Management Plan (CIMP) to document the confidential information management strategy and safeguards employed.
- Develop and deliver confidentiality and privacy onboarding training that outlines the protocols that team members must follow when accessing, storing, using, transferring, and disposing of Confidential Information and PII.
- Implement physical, administrative, and technical safeguards identified in the CIMP to proactively manage risk.
- Complete other required confidentiality and privacy training as applicable.

Deloitte also has an Insider Threat program in which Deloitte conducts active monitoring of insider threats. Insiders are defined as personnel and contractors who, based on their access to certain systems and information, could adversely affect the brand, reputation, and/or business of Deloitte or its clients. Leveraging potential risk indicators, the Insider Threat program monitors persons of interest across a broad risk spectrum, including workplace violence, espionage, fraud, and theft of intellectual property and Confidential Information. Analytic and cognitive technologies are used to help identify indicators of poor risk-culture fit and determine corresponding strategic tactics and mitigation strategies to align our sub-cultures.

## **Data Privacy**

Deloitte is committed to protecting our clients' Personally Identifiable Information (PII). Deloitte has a privacy policy, privacy notices, applicable procedures, and personnel dedicated to privacy compliance activities related to our privacy policy, privacy notices, and applicable data privacy laws and regulations. Deloitte regularly monitors for changes in privacy laws and regulations and adjust our policies and procedures when appropriate. Additionally, Deloitte maintains an annual review process across business areas to verify compliance with our privacy policies, notices, and procedures.

Deloitte has policies and procedures that protect PII and support compliance with Deloitte's legal and regulatory requirements, internal policies and procedures, and contractual obligations relating to the transfer and processing of PII.

- When Deloitte acts in the capacity of a “Business Associate” to our clients, as such role is defined under the Health Insurance Portability and Accountability Act, as amended (HIPAA), Deloitte is required to comply with the obligations of a Business Associate under HIPAA. Deloitte has implemented policies, procedures, and controls that facilitate compliance with those obligations.
- Deloitte performs an annual self-assessment process to validate adherence to data privacy lifecycle safeguards regarding the collection, use, transfer, storage, and destruction of PII for Business Processes and Service Lines that process PII.
- Deloitte utilizes a Privacy Impact Assessment (PIA) process for new systems, changes to existing systems and high-risk business processes that access, transfer or store PII.
- In support of the Privacy by Design concept, Deloitte has incorporated privacy and confidentiality requirements into our secure systems development lifecycle (SSDLC) for internally developed systems so that these requirements are considered early and often throughout the lifecycles of technology projects using a risk-based approach.
- Members of Deloitte’s Privacy team hold various security and privacy certifications (e.g., CIPP/US, CISSP).
- Deloitte assists its clients in fulfilling their data privacy obligations to respond to: (a) requests from individuals with respect to their PII processed by Deloitte; or (b) complaints relating to Deloitte’s processing of PII.

### **Confidentiality & Privacy Incident Management**

Deloitte has instituted an integrated incident response process designed to facilitate prompt reporting and resolution of incidents. Our confidentiality and privacy incident response process is characterized by the following:

- Centralized reporting of actual or suspected incidents to a Help Desk, which is available 24/7 with access via a toll-free number and online self-reporting capability available on Deloitte’s Intranet site.
- Training and awareness programs focused on helping personnel understand immediate steps to be taken in case of actual or suspected incidents.
- Established roles and responsibilities for incident management and response including involving the appropriate consultation resources across the Global Deloitte organization, as applicable to the specific matter.
- Documented processes and tools to help gather incident facts, initiate response activities in the required time frames, engage incident response teams, escalate incidents, and alert appropriate leaders, based on the nature of the specific incident.
- Consultation among the relevant parties regarding the need for a corrective action plan.

- Development, as appropriate, of action plans, including any required communications within required time frames, as well as actions to mitigate the risk of a future recurrence.
- Post-incident follow-up process to analyze root causes and integrate lessons learned.

### **Information Security Incident Management**

Deloitte has built an integrated incident response team that brings together the appropriate subject matter experts from various cross-functional disciplines to address each specific incident. The Information Security Incident Response Procedures (Procedures) describe how various types of incidents are handled. The Procedures identify key resources and communications that will take place based on various incident types. The Procedures identify to whom suspected incidents should be reported and describe the escalation path from the entry point in the process through resolution.

Security Awareness training is in place to educate Deloitte personnel of their responsibilities concerning security incidents. Each incident is logged, and the relevant facts are captured for analysis and reporting. When necessary, data related to the incident is maintained in a forensically sound manner and appropriate chain-of-custody is documented.

The incident response team has a variety of tools available to assist them in the analysis of incidents. These include standard security tools from software and hardware providers as well as commercial forensic tools specifically targeted for such matters.

Information security incident procedures are exercised annually so the Incident Response team can demonstrate proficiency and readiness. For each significant incident, a post-incident review is conducted to identify any areas for improvement as well as lessons learned. These findings are used to adjust, enhance, or improve the procedures.

### **Business Continuity Management (BCM) Program**

Deloitte takes disaster and contingency planning very seriously, including planning for events that impact its people, its facilities, and its technology. Deloitte's business continuity planning addresses issues such as, communications, travel, resource allocation, technology needs, and alternate work sites. Response procedures assess the well-being of personnel, provide for the continuity of essential business functions, and utilize recovery procedures for the restoration of critical business processes. These critical business processes are identified during a business impact analysis process and are documented in the business continuity plans for each business and enabling area.

Plans are designed to maximize the availability of personnel and resources to continue operations. Deloitte recognizes the importance of testing key recovery strategies to validate the effectiveness of plans. As such, annual testing is conducted and includes:

- Tabletop exercises with identified local crisis management teams
- Emergency notification system testing multiple times throughout the year

- Testing of technology systems and applications as described in the “Disaster Recovery Management Program” below
- Work from home scenarios for relevant sites

Cross-functional teams are identified to manage potential disruptive events, emergency situations, or disasters. Each Deloitte office has a local crisis management team to handle smaller, localized events impacting a single location. For larger events or those that are not specific to a single location or geography, an experienced National Incident Support Team is assigned. A National Crisis Council handles incidents that rise to the level of a true crisis requiring strategic involvement and decision-making.

Cross-functional teams are identified and documented in the plans to include representation of key stakeholders from the following areas:

- Client Services
- Office Services/Operations/Facilities
- Office of Security
- Human Resources and Benefits
- Information Technology Services
- Procurement and Travel
- Communications
- Risk Management

Deloitte has designed an impact-driven approach, which focuses on the impacts of an event, emergency, or crisis, rather than specific scenarios. Each type of situation could have an impact on our people, our facilities, our technology, or our clients. Each type of situation could require communications, whether internal or external. The team-based, impact-driven approach utilized by Deloitte provides the appropriate resources to assess and address the impacts of an event.

Deloitte’s planning considers the potential impacts and continuity of operations in the event of a pandemic, which includes a pandemic-specific governance model and response triggers. Pandemic planning and response are aligned with the crisis management and business continuity processes, including the use of the National Incident Support Team, supplemented by additional members during a pandemic response. Potential pandemic developments are monitored; identified crisis teams oversee implementation of specific pandemic action steps based on the severity of the pandemic, including targeted communications that are issued internally and externally, and the identification of critical people and resources.

### **Disaster Recovery (DR) Management Program**

Deloitte maintains an active disaster recovery management program which helps Deloitte to continue delivering information-technology-related services should a disruption occur. Deloitte’s program includes the following basic activities:

- Business continuity planning for IT infrastructure support staff.
- Business impact assessments to help define criticality of processes and systems related to recovery time objective.
- Disaster recovery planning of our technology through multiple failover capabilities.
- Implementation of resilient architectures where technology allows.
- Risk assessments as part of continual service improvement, with countermeasures identified and implemented for the newest scenarios.
- Internal review process for maintaining the quality of plans and services.

The Business Continuity Management (BCM) Program and plans include emergency-response business procedures, which go into effect following the occurrence of a disaster or other unplanned interruption.

Disaster Recovery (DR) plans include technical and business contact call lists, as well as notification and escalation information and architecture diagrams. Where pertinent, third-party information is also included. Recovery time objectives and recovery point objectives are documented and tested for each plan.

BCM/DR plans for critical infrastructure are subject to review and testing every 12 months with industry standard testing methods.

Risk assessment test scenarios vary based on business sensing and technology security. Test results are reviewed and recorded.

In summary, Deloitte has a comprehensive disaster recovery and business continuity management program that is designed to provide for the continuity of essential IT business functions and critical business processes following the occurrence of a disaster or other unplanned interruption impacting Deloitte's IT infrastructure.

## **Limits of Business Continuity and Pandemic Planning**

### **Physical and Environmental Security**

Only authorized personnel with a Deloitte-issued electronic badge are granted access to Deloitte's facilities. Procedures exist for controlling visitor access and maintaining a detailed log of all visitors to the facilities. Deloitte data centers are further restricted to only those personnel with the need to access restricted areas. Data centers have the following physical security measures: security guards, man-trap doors at primary entrance, multi-factor authentication (Deloitte-issued electronic badge and biometric readers) at secondary entrance, video cameras, and sign-in and sign-out sheets for escorted visitors.

The electricity, water, and temperature controls are pre-approved for use by the facilities administrators in the data centers. Each utility has a control in place to monitor its usage and to notify an administrator in case of failure. Automatic emergency lighting is installed in areas necessary to maintain personnel safety.

Emergency exits are located at appropriate places in Deloitte facilities. Automatic fire suppression systems have been installed to protect the facilities. In data centers, the primary type of system is HFC-125 chemical-based and activated via multiple smoke detectors, and the second type of system is based on pre-action hydronic and the detection method is temperature. Master water shut-off valves are present. Temperature and humidity controls have been implemented to protect against temperature fluctuations in all areas of the data centers containing IT equipment. These systems are tested periodically in accordance with manufacturers specifications (monthly, quarterly, semi-annually, or annually).

### **Cloud Hosting**

Deloitte has arrangements with vendors who provide Deloitte with certain Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Services (IaaS), and hosting services. Deloitte selects and retains these vendors based on, among other qualities, their capability to maintain safeguards for the systems, software, and information at issue that are consistent with leading industry security practices. Deloitte requires these vendors to implement and maintain such safeguards.

Deloitte's Cloud Services (DCS) team employs a geographical hosting strategy, with availability zones and regions located within the US. Primary and secondary availability zones are segregated by geographical region, and each geographical region is supported by dedicated vendor staff.

DCS provides administrative, physical, and technical safeguards, at Layer 0, which aligns with industry standards such as ISO 27001, ISO 22301, and AICPA SSAE 18 (SOC 2).

### **Human Resources Security**

Upon hire and on a quarterly basis, personnel must agree to comply with Deloitte's policies, including those relating to information security, confidentiality, and privacy. In addition, Deloitte personnel are required to complete security awareness training during the new hire onboarding process.

### **Background Checks for U.S. Personnel**

Deloitte generally requires that background investigations be conducted for partners, principals, and employees at the time that they join Deloitte. Potential issues that are identified in the background investigation are reviewed on an individual case-by-case basis, in light of guidance from the Equal Employment Opportunity Commission and applicable federal, state, and local law. This individualized assessment includes a determination of whether the issues identified are job-related or pose a risk to Deloitte or to its employees, partners, principals, or clients. The type of background investigation

performed depends on whether the individual joining is a partner or principal and the level of the employee. While background investigations were not always performed on Deloitte personnel, and may not always have covered the same information, background investigations of Deloitte personnel in the U.S. currently include the following, at a minimum:

- Social Security Number (SSN) verification confirms a valid number and the names and addresses associated with that number
- Felony and misdemeanor conviction searches: searches of the following records for felony and misdemeanor convictions are performed for the last five years in areas of residence, work, and school:
  - Federal courts
  - County courts
  - State repositories, where the state has made one available and it is reasonably accessible
- A national criminal record database search, including the state sex offender registries
- Education confirmation: education beyond high school confirmed
- Employment confirmation: professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, such as SEC, OFAC, OIG/GSA, FDA, FBI Most Wanted, EU Terrorist Watch List, Interpol Watch List, etc.
- Professional licenses: confirm relevant professional licenses

#### **Background checks for Personnel of Deloitte entities located in India (U.S. India)**

The type of background investigation performed depends on whether the individual joining U.S. India is a partner, principal, or employee, and the level of the employee. While background investigations were not always performed on U.S. India's personnel and may not always have covered the same information, background investigations of U.S. India personnel currently include the following, at a minimum:

- Identity Verification, where possible.
- Criminal checks: check all relevant court records for a five-year period
- Education confirmation: all university level education is confirmed
- Employment confirmation: all professional employment in the last five years is confirmed
- Searches of various government and criminal sanctions lists, including India specific and global databases
- Professional licenses: confirm relevant professional licenses



## **Code of Ethics and Professional Conduct**

Deloitte has adopted a Code of Ethics and Professional Conduct (Code) for use by its personnel. It is the duty of Deloitte personnel to know, understand, and comply with this Code, and, if applicable, report any potential violations. Personnel receive periodic reminders to review the Code and must acknowledge compliance on an annual basis. The Code includes obligations around a duty to act, including reporting any potential violations, and includes a sanctions policy for those who violate the Code. A confidential and anonymous Ethics and Compliance Hotline is also available for Deloitte personnel to report issues. The hotline is accessible 24X7 by phone, online, or via mail.

## **Information Technology Risk Management**

Deloitte has a Risk Management program that monitors possible threats and vulnerabilities to information technology assets. Risk assessment(s) are performed annually and when there are significant changes to infrastructure, technology, or environment. There are several control domains defined for risk assessment which are derived from industry standard practices and frameworks. For each control domain, implemented controls are identified and tailored and their effectiveness assessed for risk management. Risks that are not at an acceptable level are remediated or mitigated.

## **Vendor Risk Management Program**

The Vendor Risk Management program is designed to reduce vendor-related risk by:

- Building a repository of acceptable vendors;
- Assessing the security posture of vendors;
- Tracking remediation of identified issues; and
- Reviewing and assisting with vendor contracts with respect to obligations relating to Deloitte's information security program.

Deloitte's ITS Cyber Security Risk and Compliance (CSRC) program is responsible for reviewing our vendors' compliance with a standard set of security requirements, based upon the type and volume of data the vendor will access, as well as the risk posed to Deloitte and our clients. As part of this process, all internal projects as well as client-facing engagements which will require the services of a third-party vendor, must be added to the Third-Party Risk Management (TPRM) gateway by the Deloitte representative seeking the vendor relationship.

The ITS Cyber Risk review is focused on third parties who will access, be provided with, store, or process Deloitte or client's data. Third parties rated as high or medium risk must complete an online security questionnaire within Deloitte's vendor assessment system, whereas third parties rated as critical risk undergo an onsite assessment. The third party will have a maximum of thirty days to complete the online questionnaire. The questions presented within the online questionnaire, as well as during the onsite assessment, cover the following security domains: Access Control, Asset Management, Business Continuity Management, Communications and Operations Management, Compliance, Human Resource Security, Information Security Incident Management, Information

Systems Acquisition Development and Maintenance, Organizational Security, Physical and Environmental Security, Risk Management, Cloud Governance and Security Policy.

Upon the third party's completion of the online questionnaire or onsite assessment (if applicable), the ITSCyber Risk and Compliance team reviews the responses provided to identify findings, which are gaps or weaknesses in the vendor's security controls. The findings are assigned remediation dates and tracked to completion by the CSRC team in collaboration with the Deloitte contact, as well as with the third party. Third Parties providing services that require access, transmitting, processing or storage of Deloitte and/or Deloitte client information must complete the online security questionnaire at onset and periodically based upon risk ranking of the vendor profile for the duration of the agreement.

## **Records Management**

Records Management is the systematic control of official records that are retained for a specified period of time and then destroyed or archived permanently. Deloitte retains and manages official records in accordance with applicable legal and regulatory requirements, professional standards, and contractual obligations.

The US Records Management Services (RMS) team partners with stakeholders across the Deloitte businesses to facilitate compliance with policies and regulations related to records retention by providing technology, tools, processes, and customer support, including but not limited to:

- Maintaining records retention policies which align with applicable legal and regulatory requirements and professional standards and provide the guidance that is the framework for mitigating records-related risks.
- Securely managing electronic and hard copy official records critical to the operation of our businesses and services to our clients, in accordance with records retention policies, including classification of official records to facilitate application of retention periods.
- Providing secure business-focused systems and processes for the retention, preservation, protection, and disposition of official records.
- Facilitating, promoting, and monitoring compliance with records-related requirements through streamlined processes and tools, compliance notifications, and reporting.
- Coordinating the proper handling of files subject to special circumstances due to legal, tax, or regulatory preservation requirements.
- Executing post-retention records destruction processes in accordance with records policies and principles.



Deloitte & Touche LLP

**Date:** May 26, 2022  
**FEIN:** 133891517

**Billing Address:**  
ATTN: Ms. Kimberly Fontan  
Entergy Texas, Inc.  
639 Loyola Avenue  
New Orleans LA 70113  
USA

For professional services rendered

---

<b>Fees</b>	<b>\$ 150,000.00</b>
Billing related to our attestation report over the Summary of Costs	
Billed by Entergy Services, LLC and Other Entergy Affiliates to Entergy	
Texas, Inc. in accordance with the Engagement Letter dated May 5, 2022	
<b>Total Amount Due (USD)</b>	<b>\$ 150,000.00</b>

## Invoice 8002650719

### Payment Instructions:

#### Check Payment Mailing Address:

Deloitte & Touche LLP  
PO Box 844708  
Dallas TX 75284-4708

#### Email remittance information to:

[deloittepayments@deloitte.com](mailto:deloittepayments@deloitte.com)

Please pay by ACH amounts and with  
CTX, CCD+ or WIRE. Include  
Invoice numbers/ your company name  
with payment.

**Bank Name:** Bank of America

#### Electronic funds payment details

**ABA# and ACH#:** 011900571  
**US WIRE:** 026009593  
**Swift Code :** BOFAUS3N  
**Account Title:** DELOITTE & TOUCHE  
LLP  
**Account Number:** 385015866213

#### Payment Terms:

Per Contract or Upon Receipt

#### Billing Office:

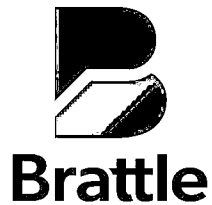
701 Poydras Street  
Suite 4200  
New Orleans LA 70139-4200

#### Sold to Address:

ENTERGY CORPORATION  
639 Loyola Ave  
NEW ORLEANS LA 70113-3125

#### Overnight Mailing Address:

Deloitte & Touche LLP LBX# 844708  
1950 N. Stemmons Freeway  
Suite 5010  
Dallas TX 75207



Mr. Michael A. Boldt, Esq.  
michaelboldt@eversheds-sutherland.com  
Eversheds Sutherland (US) LLP  
One American Center  
600 Congress Avenue  
Suite 2000  
Austin, TX 78701

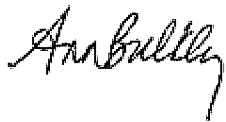
June 6, 2022

Re: ETI Rate Case

Dear Michael,

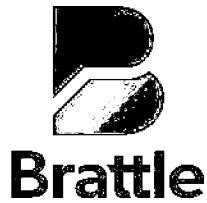
Attached please find our invoice for work performed in April 2022 on the matter referenced above. Please let me know if you have any questions relating to this invoice or our work.

Sincerely,



**Ann Bulkley**  
**PRINCIPAL | BOSTON**

JR



May 31, 2022

In Account With:

Michael Boldt  
Eversheds Sutherland LLP  
600 Congress Avenue  
Suite 2000  
Austin TX 78701  
United States

Invoice Number 067393  
ProjectID CL-07867  
Page 1 of 1

*For Professional Services Rendered Through April 30, 2022*

	<u>Hours</u>	<u>Rate</u>	<u>Amount</u>
<u>Principals</u>			
Ann Bulkley-Armour	2.75	625.00	1,718.75
<u>Senior Associate</u>			
Christopher Wall	4.00	475.00	1,900.00
<u>Modeling Specialist</u>			
Andrew Thompson	0.50	315.00	157.50
<u>Research &amp; Litigation Analysts</u>			
Mingzhe Shao	5.00	375.00	1,875.00
Ethan Snyder	1.50	250.00	375.00
Total Labor			<u>\$6,026.25</u>
<b>TOTAL LABOR &amp; EXPENSES</b>			<b><u>\$6,026.25</u></b>

Please note our updated banking information below. For additional information contact [accountsreceivable@brattle.com](mailto:accountsreceivable@brattle.com).

Payable upon receipt in US Dollars to: The Brattle Group, Inc. (FID 04-3254813)

Finance Charge of 1.5% per month (18% APR) will be added to overdue invoices.

Please Remit Payment as Follows:

**Check Payments:**

The Brattle Group, Inc.  
One Beacon Street, Suite 2600  
Boston, MA 02108

**ACH/Wire Payments:**

Citibank, N.A. New York  
SWIFT No.: CITIUS33  
ABA No.: 021000089  
Account: BRATTLE GROUP - OPERATING  
Account No.: 31240031

**Telephone:**

+1.617.864.7900

**Email:** [billingdept@brattle.com](mailto:billingdept@brattle.com)

Project: CL07867  
April 1 - April 30, 2022  
Time Log for Bulkley-Armour, Ann

Date	Description of Activity/Tasks	Hours
04/05/22	Updated proxy group screening for March data.	1.00
04/06/22	Reviewed model results. Updates to testimony. Conf. call to discuss current model results.	1.75
<b>TOTAL</b>		<b>2.75</b>

Project: CL07867  
April 1 - April 30, 2022  
Time Log for Wall, Christopher

Date	Description of Activity/Tasks	Hours
04/01/22	Updated the ROE model. Reviewed the exhibits.	0.75
04/04/22	Updated the exhibits.	1.00
04/05/22	Reviewed and updated the exhibits.	2.25
<b>TOTAL</b>		<b>4.00</b>

Project: CL07867  
April 1 - April 30, 2022  
Time Log for Thompson, Andrew

Date	Description of Activity/Tasks	Hours
04/26/22	Worked on testimony.	0.50
TOTAL		0.50



Project: CL07867  
April 1 - April 30, 2022  
Time Log for Shao, Mingzhe

Date	Description of Activity/Tasks	Hours
04/04/22	Updated exhibits with March data.	4.25
04/05/22	Reviewed exhibits.	0.75
TOTAL		5.00

Project: CL07867  
April 1 - April 30, 2022  
Time Log for Snyder, Ethan

Date	Description of Activity/Tasks	Hours
04/01/22	Worked on ROE model update.	1.00
04/29/22	Worked on ROE model update.	0.50
TOTAL		1.50



A: 4930 Trail West Drive  
Austin, TX 78735

P: 512-800-2664

E: [totten@ospreyenergy.com](mailto:totten@ospreyenergy.com)

W: [www.ospreyenergy.com](http://www.ospreyenergy.com)

## INVOICE

**Invoice No. ETI-RC 2022-1**

Date: May 3, 2022

To: Michael Boldt, Eversheds, Sutherland

Invoice for Services		
Date	Description	Hours
	Services provided pursuant to Letter Agreement between Eversheds, Sutherland and Osprey Energy Group:	
March 8	Call with Eversheds, Sutherland, ETI, research	1.0
March 9	Research	0.25
April 6	Call with Eversheds, Sutherland, ETI	1.5
April 8	Research	2.75
April 11	Draft testimony	1.75
April 13	Review testimony	0.5
April 25	Draft testimony	1.25
April 29	Draft testimony	1.5
<b>Total Hours</b>		<b>10.5</b>
<b>Billing Rate is \$350</b>		<b>Total Amount Due \$3,675.00</b>
<p>Please contact Jess Totten if there are any questions concerning this invoice. 512-800-2664</p> <p>Please remit payment to:</p> <p>Osprey Energy Group 4930 Trail West Drive Austin, Texas 78767</p> <p>Tax ID No. 32-0545549</p>		

May 17, 2022

Timothy Lyons  
ScottMadden, Inc.  
2626 Glenwood Ave., Suite 480  
Raleigh, NC 27608

Dear Mr. Lyons:

This Letter Agreement sets forth the terms and conditions of the agreement between ScottMadden, Inc. ("Consultant") and Eversheds Sutherland (US) LLP ("Sutherland") concerning the provision of professional consulting services by Consultant to assist Sutherland and its client, Entergy Texas, Inc. ("ETI" or "client"), in connection with administrative litigation before the Public Utility Commission of Texas ("Commission") for ETI's base rate case to be filed in 2022.

1. The terms of this Letter Agreement shall be effective as of the date first written above, and shall continue until a final order is issued by the Commission in the above referenced ETI rate case or until terminated sooner by mutual agreement.

2. SERVICES TO BE PERFORMED: Consultant shall serve as a consulting expert to Sutherland and shall advise and consult with Sutherland and perform services as requested in connection with the administrative litigation referenced above. Such services shall include the production of pre-filed written testimony regarding regulatory policy for ETI to be filed in the litigation as well as participation in discovery and the provision of live testimony in that matter.

3. CONSIDERATION: Consultant shall be entitled to compensation for authorized professional services and reimbursement for authorized expenses incurred in the performance of authorized services at the rate of \$470 per hour for work performed during April 2022 and \$365 per hour for work performed May 2022 forward. Consultant shall submit invoices for fees and expenses (with supporting data) once a month, and such invoices shall be due and payable within sixty (60) days after receipt thereof.

4. INDEPENDENT CONTRACTOR: It is understood and agreed that Consultant is an independent contractor and not an agent, employee, or representative of Sutherland or its client in the litigation.

5. CONFIDENTIALITY: The services provided by Consultant and the products of such services that Consultant will be providing pursuant to this Letter Agreement are strictly confidential, are privileged attorney work-product, and are further protected by all applicable privileges and exemptions specified in the pertinent Texas and Federal Rules of Civil Procedure and related administrative procedural rules. Except as otherwise required by law or regulation, any and all documentation, data, opinions, information, and communications heretofore or hereafter made or furnished by Sutherland or its client in the litigation to Consultant in connection with its providing services under this Letter Agreement shall remain proprietary to Sutherland, shall be held by Consultant in strict confidence and subject to the aforementioned privileges and exemptions while in the possession of Consultant, shall not be released or disclosed by Consultant without the prior written consent of Sutherland, and shall be returned upon request to Sutherland at such time as

Consultant no longer has a need to retain same in the course of providing services to Sutherland or at such other time as Sutherland may specify. Except as otherwise required by law, regulation, or court order, any and all documentation, data, opinions, information, and communications made or developed by Consultant with or as a part of the services provided to Sutherland shall be held by Consultant and in strict confidence and subject to the aforementioned privileges and exemptions, and shall not be released or disclosed by Consultant to any third party without the prior written consent of Sutherland.

6. OWNERSHIP OF MATERIAL: It is understood and agreed that all materials in written, graphic, electronically-stored or other form, generated or prepared in the course of providing services to Sutherland pursuant to this Letter Agreement, together with all copyrights therein, shall belong to Sutherland and its client. Consultant agrees to assign to Sutherland and its client all right, title, interest in all such materials, and agrees to execute any documents reasonably necessary for Sutherland and its client to perfect its ownership interests. Notwithstanding the foregoing, Consultant shall be permitted to retain for its records one copy of all materials involved in the provision of service to Sutherland pursuant to this Letter Agreement.

7. CONFLICT OF INTEREST: Due to the privileged and confidential nature of the information supplied by Sutherland and its client in the litigation to Consultant in accordance with this Letter Agreement, it is understood and agreed that absent prior written consent of Sutherland which will not be unreasonably withheld, neither Consultant nor its agents, employees or subcontractors shall, at any time hereafter, contract with or otherwise become employed by, serve, or provide advice to any individual or entity other than Sutherland, or its client in the litigation, in connection with any matter adverse to ETI where Consultant could make use of privileged and confidential information acquired in connection with the litigation.

8. SUTHERLAND OBLIGATIONS: Consultant acknowledges and agrees that Sutherland has been retained to serve as legal counsel for its client in connection with the litigation, and any and all fees and expenses to be paid to Consultant are ultimately the responsibility of the client.

9. ENTIRE AGREEMENT: It is understood and agreed that this Letter Agreement constitutes the entire agreement between Sutherland and Consultant regarding the provision of litigation support services. There are no promises, agreements, conditions, or understandings by and between Sutherland and Consultant that are not set forth herein.

The foregoing accurately states the agreement between Consultant and Sutherland concerning the matters set forth herein.

**EVERSHEDS SUTHERLAND (US) LLP**

By: \_\_\_\_\_

  
**Michael Boldt**  
**For the Firm**

ACCEPTED AND AGREED TO BY  
ScottMadden, Inc.

By: Logan Toms

Its: Partner, Finance and Risk

Date: 5/18/22

Table 1: Proposed Schedule of Hourly Professional Fees

Position	Rate
Partner	\$470.00
Director	\$365.00
Manager	\$340.00
Senior Associate	\$300.00
Associate	\$255.00
Senior Analyst	\$170.00
Analyst	\$145.00
Administrative Assistant	\$65.00



Smart. Focused. Done Right.

**ScottMadden, Inc.**  
2626 Glenwood Avenue  
Suite 480  
Raleigh, NC 27608  
919-781-4191  
scottmadden.com

May 23, 2022

Invoice Number: 020950

Michael Boldt  
Eversheds Sutherland (US) LLP  
600 Congress Avenue  
Suite 2000  
Austin, TX 78701

In Reference To: Professional services provided in April 2022 for project 364-005  
Entergy Texas Benchmarking

---

	<i>Amount</i>
<b>Professional Fees</b>	\$ 3,370.00
<b>Total Fees and Expenses</b>	<u>\$ 3,370.00</u>
<b>Total Due</b>	<u><u>\$ 3,370.00</u></u>

If you have any questions regarding this invoice, please let me know. Please remit payment in U.S. funds to:  
ScottMadden, PO Box 935955, Atlanta, GA 31193-5955. Thank you for retaining ScottMadden.

Sincerely,

A handwritten signature in black ink that reads "R Starkweather".

Richard D. Starkweather, IV  
Partner

ScottMadden, Inc.  
Tax ID: 56-1445505

May 23, 2022  
Page 2

In Reference To: Professional services provided in April 2022 for project 364-005  
Entergy Texas Benchmarking

**Professional Fees Summary**

	<i>Hours</i>	<i>Rate</i>	<i>Amount</i>	
Richard D. Starkweather, IV	5.00	470	\$	2,350.00
Quentin Watkins	4.00	255	\$	1,020.00
			\$	<u>3,370.00</u>



**ScottMadden, Inc.**

Time & Expense Detail

---

<b>Client Name:</b>	<b>Eversheds Sutherland LLP</b>	<b>Invoice #:</b>	<b>020950</b>
<b>Project:</b>	<b>364-005- Entergy Texas Benchmarking</b>		

---

099 Richard D. Starkweather, IV

Billable Time:		<u>Units</u>	<u>Rate</u>	<u>Amount</u>
4/18/2022	Richard D. Starkweather, IV	2.00	470.000	\$940.00
4/19/2022	Richard D. Starkweather, IV	1.00	470.000	\$470.00
4/26/2022	Richard D. Starkweather, IV	1.00	470.000	\$470.00
4/29/2022	Richard D. Starkweather, IV	1.00	470.000	\$470.00
Total Billable Time:		5.00		\$2,350.00
Total for Richard D. Starkweather, IV:				\$2,350.00

**ScottMadden, Inc.**

Time & Expense Detail

---

<b>Client Name:</b>	<b>Eversheds Sutherland LLP</b>	<b>Invoice #:</b>	<b>020950</b>
<b>Project:</b>	<b>364-005- Entergy Texas Benchmarking</b>		

---

295            Quentin Watkins

<u>Billable Time:</u>		<u>Units</u>	<u>Rate</u>	<u>Amount</u>
4/15/2022	Quentin Watkins	1.00	255.000	\$255.00
4/18/2022	Quentin Watkins	2.00	255.000	\$510.00
4/26/2022	Quentin Watkins	1.00	255.000	\$255.00
Total Billable Time:		4.00		\$1,020.00
Total for Quentin Watkins:				\$1,020.00



Smart. Focused. Done Right.

**ScottMadden, Inc.**

2626 Glenwood Avenue

Suite 480

Raleigh, NC 27608

919-781-4191

scottmadden.com

June 23, 2022

Invoice Number: 021107

Michael Boldt  
Eversheds Sutherland (US) LLP  
600 Congress Avenue  
Suite 2000  
Austin, TX 78701

In Reference To: Professional services provided in May 2022 for project 364-005  
Entergy Texas Benchmarking

---

	<i>Amount</i>
<b>Professional Fees</b>	\$ 19,200.00
<b>Total Fees and Expenses</b>	<u>\$ 19,200.00</u>
<b>Total Due</b>	<u><u>\$ 19,200.00</u></u>

If you have any questions regarding this invoice, please let me know. Please remit payment in U.S. funds to:  
ScottMadden, PO Box 935955, Atlanta, GA 31193-5955. Thank you for retaining ScottMadden.

Sincerely,

A handwritten signature in black ink, appearing to read "R Starkweather".

Richard D. Starkweather, IV  
Partner

ScottMadden, Inc.  
Tax ID: 56-1445505

June 23, 2022  
Page 2

In Reference To: Professional services provided in May 2022 for project 364-005  
Entergy Texas Benchmarking

### Professional Fees Summary

	<i>Hours</i>	<i>Rate</i>	<i>Amount</i>
Quentin Watkins	8.00	255	\$ 2,040.00
Javaris Blue	12.00	255	\$ 3,060.00
Rick Starkweather	30.00	470	\$ 14,100.00
			<hr/>
			\$ 19,200.00

**ScottMadden, Inc.**

Time & Expense Detail

---

<b>Client Name:</b>	<b>Eversheds Sutherland LLP</b>	<b>Invoice #:</b>	<b>021107</b>
<b>Project:</b>	<b>364-005- Entergy Texas Benchmarking</b>		

---

295            Quentin Watkins

<u>Billable Time:</u>		<u>Units</u>	<u>Rate</u>	<u>Amount</u>
5/2/2022	Quentin Watkins	4.00	255.000	\$1,020.00
5/3/2022	Quentin Watkins	1.00	255.000	\$255.00
5/4/2022	Quentin Watkins	1.00	255.000	\$255.00
5/6/2022	Quentin Watkins	1.00	255.000	\$255.00
5/10/2022	Quentin Watkins	1.00	255.000	\$255.00
	Total Billable Time:	8.00		\$2,040.00
	Total for Quentin Watkins:			\$2,040.00

**ScottMadden, Inc.**

Time & Expense Detail

---

<b>Client Name:</b>	<b>Eversheds Sutherland LLP</b>	<b>Invoice #:</b>	<b>021107</b>
<b>Project:</b>	<b>364-005- Entergy Texas Benchmarking</b>		

---

777	Javaris Blue			
Billable Time:		<u>Units</u>	<u>Rate</u>	<u>Amount</u>
5/17/2022	Javaris Blue	8.00	255.000	\$2,040.00
5/18/2022	Javaris Blue	4.00	255.000	\$1,020.00
Total Billable Time:		<u>12.00</u>		<u>\$3,060.00</u>
Total for Javaris Blue:				<u>\$3,060.00</u>

**ScottMadden, Inc.**

Time & Expense Detail

---

<b>Client Name:</b>	<b>Eversheds Sutherland LLP</b>	<b>Invoice #:</b>	<b>021107</b>
<b>Project:</b>	<b>364-005- Entergy Texas Benchmarking</b>		

---

X08 Rick Starkweather

Billable Time:		<u>Units</u>	<u>Rate</u>	<u>Amount</u>
5/2/2022	Rick Starkweather	6.00	470.000	\$2,820.00
5/3/2022	Rick Starkweather	2.00	470.000	\$940.00
5/4/2022	Rick Starkweather	2.00	470.000	\$940.00
5/5/2022	Rick Starkweather	2.00	470.000	\$940.00
5/6/2022	Rick Starkweather	3.00	470.000	\$1,410.00
5/8/2022	Rick Starkweather	2.00	470.000	\$940.00
5/9/2022	Rick Starkweather	4.00	470.000	\$1,880.00
5/10/2022	Rick Starkweather	3.00	470.000	\$1,410.00
5/11/2022	Rick Starkweather	1.00	470.000	\$470.00
5/15/2022	Rick Starkweather	1.00	470.000	\$470.00
5/16/2022	Rick Starkweather	2.00	470.000	\$940.00
5/17/2022	Rick Starkweather	1.00	470.000	\$470.00
5/18/2022	Rick Starkweather	1.00	470.000	\$470.00
Total Billable Time:		<hr/> 30.00		<hr/> \$14,100.00
Total for Rick Starkweather:				<hr/> \$14,100.00

The following files are not convertible:

Exhibits MEG-SD1-1 through MEG-SD1-  
17.XLSX

Please see the ZIP file for this Filing on the PUC Interchange in order to access these files.

Contact [centralrecords@puc.texas.gov](mailto:centralrecords@puc.texas.gov) if you have any questions.