DOCKETED	
Docket Number:	01-AFC-07C
Project Title:	01-AFC-7C Russell City Energy Company
TN #:	242288
Document Title:	Russell City Energy Center Application for Confidential Designation (Supplemental)
Description:	N/A
Filer:	Deric Wittenborn
Organization:	Ellison Schneider Harris & Donlan LLP
Submitter Role:	Applicant Representative
Submission Date:	3/11/2022 4:42:38 PM
Docketed Date:	3/11/2022

March 11, 2022

Drew Bohan
Executive Director
California Energy Commission
1516 Ninth Street
Sacramento, CA 95814

Re: Russell City Energy Center (01-AFC-07C): Application for Confidential Designation (Supplemental)

Dear Mr. Bohan:

Per our discussions with California Energy Commission Chief Counsel, the Russell City Energy Company, LLC hereby submits this supplemental Application for Confidential Designation on behalf of the Russell City Energy Center.

Please contact me at 916-447-2166 or jdh@eslawfirm.com should you have any questions or require additional information. Thank you.

Sincerely,

Jeffery D. Harris
Ellison Schneider Harris & Donlan LLP
2600 Capitol Avenue, Suite 400
Sacramento, CA 95816
Tel: (916) 447-2166
Email: jdh@eslawfirm.com

Attorneys for Russell City Energy Company, LLC

cc: Linda Barrera, CEC Chief Counsel

APPLICATION FOR CONFIDENTIAL DESIGNATION
Russell City Energy Center (01-AFC-07C)

1. Specifically indicate those parts of the record which should be kept confidential.

a. Title, date, and description (including number of pages) of the information or data for which you request confidential designation.

Russell City Energy Company, LLC ("Applicant") seeks confidential designation for the following documents prepared by or at the direction of the Applicant, Calpine Corporation, Calpine Operating Services Company, Inc. ("COSCI") and affiliated entities (collectively, "Site Inspection Documents") submitted to California Energy Commission staff on behalf of the Russell City Energy Center ("RCEC"):

Folder Title[1]	Document Description
1. COVID-19 SAFETY PROTOCOLS	Pandemic Guide for Power Operations
3. SPILL PREVENTION CONTROL AND COUNTERMEASURES (SPCC) PLAN	SPCC Plan
5. FIRE PROTECTION SYSTEMS	07-Fire Protection Plan
7. JOB SAFETY HAZARD ANALYSIS	Job Safety Analysis Standard
	Safe Work Permit Samples
8. HOT WORK PERMITS	Hot Work Permit Procedure
	Hot Work Permits- Samples
9. CONFINED SPACE PERMITS	RCEC Combined Space Entry Standard
	Confined Space Permits Sample
10. LOCKOUT TAGOUT PERMITS	Lockout Tagout Standard
	LOTO 3068, 3069, 3070
11. GENERATOR STEP UP MAINTENANCE DOCUMENTATION	Maintenance Plan—EDG-104 Calpine Transformer Reliability Program
	Annual Inspection Reports
	Dissolved Gas in Oil Analysis Report
12. PERSONAL PROTECTIVE EQUIPMENT	Personal Protective Equipment Standard

b. Parts of the information or data for which you request confidential designation.

The Site Inspection Documents should be kept confidential in their entirety. In particular, personnel information such as names, phone numbers, and email addresses must be kept

[1] "Folder Title" refers to the corresponded file directory folder that the Site Inspection Documents were uploaded to in accordance with directions received from California Energy Commission Staff.

confidential, as should control room information and other detailed information regarding the facility. Publicly available operational information can facilitate attacks on energy infrastructure, such as the RCEC, by providing access to known or potential vulnerabilities.

2. State the length of time the record should be kept confidential and provide justification for the length of time.

The Site Inspection Documents should be kept confidential for the operating life of the RCEC.

3. Cite and discuss:

(a) the provisions of the Public Records Act or other law that allow the Commission to keep the information or data confidential, and explain why the provision applies to the material; and

(b) the public interest in nondisclosure of the material submitted for confidential designation. If the material contains trade secrets or its disclosure would otherwise cause loss of a competitive advantage, please state how it would be lost, the value of the information to the applicant and the ease or difficulty with which the information could be legitimately acquired or duplicated by others.

GENERALLY APPLICABLE PROVISIONS

Several federal and state laws exempt from disclosure the Site Inspection Documents.

Trade Secret

The Public Records Act ("PRA") exempts from disclosure "[r]ecords, the disclosure of which is exempted or prohibited pursuant to federal or state law." (Govt. Code § 6254(k).) Evidence Code section 1060 provides that "the owner of a trade secret has a privilege to refuse to disclose the secret, and to prevent another from disclosing it, if the allowance of the privilege will not tend to conceal fraud or otherwise work injustice." Trade secrets is defined as "information, including a formula, pattern, compilation, program, device, method, technique, or process that: (1) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." (Civ. Code § 3426.1(d).) Corporate proprietary information, including trade secrets, is similarly exempted from public disclosure pursuant to the PRA. (For example, see Govt. Code §§ 6254.7(d), 6254.15.)

The Site Inspection Documents contain the specific operating procedures, programs, and generating processes employed at the RCEC that govern the efficient, reliable, and safe operation and generation of electricity at the facility. The Site Inspection Documents contain confidential and proprietary business information such as facility operational procedures, how risks are assessed at the facility, the status of facility equipment, vulnerability information, and operational parameters for certain facility components and other commercially valuable information related to the facility's operations and potential improvements.

The Applicant has invested significant resources in the creation and refinement of the Site Inspection Documents. The Applicant derives independent economic value from the Site Inspection Documents not being generally known to either the public or to competitors. The Site Inspection Documents are neither publicly available nor obtainable unless employed or contracted by the Applicant or its affiliated entities. Further, contractors are only provided access to certain Site Inspection Documents on a need-to-know basis and are not allowed to otherwise copy or remove the Site Inspection Documents from the RCEC. The efficient and reliable operation of the RCEC in accordance with the Site Inspection Documents affects the maintenance and operational costs of the facility, which in turn directly correlates to economic value for the Applicant.

If made publicly available, Applicant's competitors would have access to the specific operating procedures, programs, and generating processes employed at the RCEC, in addition to the status and condition of facility equipment. Competitors can obtain economic value from the disclosure of the Site Inspection Documents, as they would have access to operational manuals, processes, and other information that can be used to streamline or benefit the power plant operations of competitors, ascertain operational and maintenance needs, which in turn affects operational and maintenance costs. Furthermore, disclosure would allow competitors to utilize information regarding power plant operations and proceedings that the Applicant has put a significant amount of time and resources in developing in a manner for free. This would put the RCEC at a further competitive disadvantage as the Applicant would not have access to similar levels of information regarding its competitors because such detailed operating information regarding power plants operations such as that contained in the Site Inspection Documents are not typically made public.

Plant Production Data and Similar Information Relating to Utility Systems Development

The PRA exempts from disclosure "[g]eological and geophysical data, plant production data, and similar information relating to utility systems development, or market or crop reports, that are obtained in confidence from any person." (Govt. Code § 6254(k).) The Site Inspection Documents include production data, in addition to similar information regarding the development and maintenance of the RCEC and were provided in confidence to CEC staff as part of the site inspection of the RCEC. The Site Inspection Documents are thus exempt from disclosure under Section 6254(k) of the PRA.

Personnel Information

The PRA exempts from disclosure "[p]ersonnel, medical, or similar files, the disclosure of which would constitute an unwarranted invasion of privacy." (Gov't Code § 6254(c).) Because the Site Inspection Documents contain employee names, positions, contact information, and other information that if released would constitute an unwarranted invasion of privacy and potentially interfere with the performance of duties by critical infrastructure workers, such information is exempt from disclosure under the PRA.

Such protections are particularly important, given emerging threats of cyber security where employees names and credentials are "spoofed" for exploitation. Ransomware, trojans, spyware,

viruses, worms, and any other type of attack that leverages software in a malicious way most often uses employee names to help design illicit entry methods.

Public Interest in Nondisclosure

The PRA provides a specific exclusion from disclosure where "…on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record." (Govt. Code § 6255(a).) The public interest served by not disclosing the Site Inspection Documents clearly outweighs the public interested served by disclosure as nondisclosure will protect against potential misuse of the information for illicit purposes, such as vandalism, tampering, or other third-party imposed damages.

Attacks on energy infrastructure are a real, contemporary threat. In recent years, high-powered rifles were used to destroy power transformers at a substation in California, and attacks to physical electric infrastructure, such as power plants, remain a concern.[2] As documented in the most recent National Terrorism Advisory System ("NTAS") Bulletin published on February 7, 2022:

> While the conditions underlying the heightened threat landscape have not significantly changed over the last year, the convergence of the following factors has increased the volatility, unpredictability, and complexity of the threat environment: (1) the proliferation of false or misleading narratives, which sow discord or undermine public trust in U.S. government institutions; (2) continued calls for violence directed at U.S. critical infrastructure…[3]

The NTAS Bulletin further explains that "Domestic violent extremists have also viewed attacks against U.S. critical infrastructure as a means to create chaos and advance ideological goals and have recently aspired to disrupt U.S. electric and communications critical infrastructure, including by spreading false or misleading narratives about 5G cellular technology."[4]

Attacks are not limited to direct physical attacks but can involve cyber attacks and influence operations. On February 18, 2022, the Cybersecurity & Infrastructure Security Agency ("CISA") released information describing the increasing "risk and potency of influence operations to U.S. critical infrastructure" that have the specific goal of disrupting U.S. critical

[2] U.S. Department of Homeland Security and Cybersecurity & Infrastructure Security Agency, *Energy Sector-Specific Plan*, pp. 15-16 (2015), available at: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

[3] U.S. Department of Homeland Security, National Terrorism Advisory System Bulletin (February 7, 2022), available at: https://www.dhs.gov/sites/default/files/ntas/alerts/22_0207_ntas-bulletin.pdf.

[4] U.S. Department of Homeland Security, National Terrorism Advisory System Bulletin (February 7, 2022), available at: https://www.dhs.gov/sites/default/files/ntas/alerts/22_0207_ntas-bulletin.pdf.

infrastructure and undermine U.S. interests and authorities.[5] Hacking and other cyber activities may be used to attack infrastructure.[6]

In January 2022 and in a March 2022 update, CISA reported on Russian-based hackers targeting the energy sector.[7] These Russian state-sponsored advanced persistent threat ("APT") actors conducted a multi-stage intrusion campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data."[8] CISA reports "The threat actors in this campaign employed a variety of [tactics, techniques, and procedures] TTPs, including: spear-phishing emails (from compromised legitimate account), watering-hole domains, credential gathering, open-source and network reconnaissance, host-based exploitation, and targeting industrial control system (ICS) infrastructure."[9] As CISA explained, "In multiple instances, the threat actors accessed workstations and servers on a corporate network that contained data output from control systems within energy generation facilities. The threat actors accessed files pertaining to [industrial control system] ICS or supervisory control and data acquisition (SCADA) systems. Based on DHS analysis of existing compromises, these files were named containing ICS vendor names and ICS reference documents pertaining to the organization (e.g., "SCADA WIRING DIAGRAM.pdf" or "SCADA PANEL LAYOUTS.xlsx")."[10] These threats are not hypothetical or amorphous, but are a real, contemporary concern.

Title 6, section 131 of the U.S. Code defines "critical infrastructure information" as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems," such as information relating to the "ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation," and including security testing, risk evaluation, risk management planning, or risk audit, or information relating to "any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation." Section 131 also defines the term "protected systems" to include "any service, physical or computer-based system, process, or procure that directly or indirectly affects the viability of a facility of critical structure."

---

[5] CISA, *Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure* (February 2022), https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf.

[6] CISA, *Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure* (February 2022), https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf.

[7] CISA, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure* (March 1, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-011a.

[8] CISA, *Alert (AA22-011A), Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, (Original release date: January 11, 2022; last revised: March 01, 2022), https://www.cisa.gov/uscert/ncas/alerts/aa22-011a.

[9] CISA, *Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors* (Original release date, March 15, 2018, Last revised: March 16, 2018), https://www.cisa.gov/uscert/ncas/alerts/TA18-074A.

[10] *Id.*

Publicly available operational information and CII can facilitate attacks on energy infrastructure, such as the RCEC, by providing access to known or potential vulnerabilities. The Site Inspection Documents do not simply give the general location of the critical infrastructure. The Site Inspection Documents contain specific engineering, vulnerability, operational procedures, or detailed design information regarding the generation of electricity at the RCEC.

While each document standing alone may not pose a concern if publicly disclosed, the entire set of Site Inspection Documents as a whole provide a comprehensive picture regarding operation of the RCEC. These documents outline how plant personnel make decisions, respond to events at the facility, the process to identify and repair the facility, identify key facility, and company personnel, provide contact information for personnel, and even provide details for how access to the facility occurs. Given the detailed operating procedures and information, the Site Inspection Documents could be useful to a person planning an attack on critical infrastructure.

The Site Inspection Documents also provide details regarding plant personnel include names, positions, responsibilities, and contact information. The public interest in nondisclosure of such information is to reduce the risk of influence operations, phishing, or other hacking attacks from identifying and targeting key plant personnel.

Finally, as recognized by CISA, "Information on vulnerabilities, threats, and consequences is, by nature, sensitive" and that "Unless both public and private sector partners trust that shared information will be strictly protected and used only for agreed-upon purposes, the costs of sharing sensitive information could be seen to outweigh the benefits, and the partnership could fail."[11] The public interest in nondisclosure in this case is to facilitate the continued information sharing between the public and private sector. Further, there are alternative means for the public to be informed about the safe operation of power plants. The Applicant submits an Annual Compliance Report ("ACR") that provides a public summary of the facility's operations and details regarding the facility's compliance with both its certification and laws, ordinances, regulations, and standards ("LORS").

Copyright

Federal law provides copyright protections for original works of authorship in literary works. (17 U.S.C. § 102.) Literary works are "works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied." (17 U.S.C. § 101.) As described above, the Site Inspection Documents are original works created by or on behalf of the Applicant, which express in words the methods to operate and maintain the RCEC. Therefore, the Site Inspection Documents cannot be copied, be publicly posted, or reproduced without the express written permission of the Applicant.

[11] U.S. Department of Homeland Security and Cybersecurity & Infrastructure Security Agency, *Energy Sector-Specific Plan*, p. 23 (2015), available at: https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

APPLICATION FOR CONFIDENTIAL DESIGNATION
Russell City Energy Center (01-AFC-07C)

SPECIFIC PROVISIONS APPLICABLE TO EACH DOCUMENT

In addition to the general provisions discussed above, the specific provisions of law and rationales for keeping the Site Inspection Documents confidential are discussed below in detail for each document listed in Section 1 above.

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
1. COVID-19 SAFETY PROTOCOLS	Pandemic Guide for Power Operations	**Site Security/Vulnerability Concerns** The Pandemic Guide for Power Operations contains information regarding the procedures for access to the site that should not be made public. **Personnel Information/ Proprietary Business Information** The Pandemic Guide for Power Operations also contains internal email information, vendors used by the Applicant, personnel information, and vendor ordering information. This information should not be publicly disclosed.
3. SPILL PREVENTION CONTROL AND COUNTERMEASURES (SPCC) PLAN	SPCC Plan	**Site Security/Vulnerability Concerns** The SPCC Plan contains facility-specific information that discloses detailed information regarding all petroleum products on the site. The scope of the information within the SPCC Plan far exceeds what is publicly available through the public information contained in CEC licensing documents. In particular, the SPCC Plan includes detailed locations of where all regulated substances are stored, the equipment that uses regulated substances, potential failure vulnerabilities, amounts of regulated substances, site security and access measures, and specific operational procedures that detail how regulated substances are handled. This information is similar in nature to the Risk Management Plan that was previously granted confidential designation.[12] **Personnel Information** The SPCC Plan contains personnel information, including personnel names, contact information, and

[12] TN#: 241378, p. 5.

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
		other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The SPCC Plan, including the Appendices, are documents and materials that were either created directly by the Applicant or on the Applicant's behalf. The Applicant has invested substantial time and resources to the creation of the SPCC Plan, including the time and research necessary to research applicable LORS, development of specific procedures to manage regulated substances and respond to incidents, and development of internal checklists and forms to encapsulate the site-specific procedures.
5. FIRE PROTECTION SYSTEMS	07-Fire Protection Plan	**Site Security/Vulnerability Concerns** The Fire Protection Plan contains facility-specific information that discloses detailed information regarding the facility's fire system; maintenance, testing, and inspection procedures; and facility response should a fire occur at the site. The Fire Protection Plan provides details regarding the ability of the facility to resist compromise or incapacitation from fire and should not be disclosed. **Trade Secret/Business Information** The Fire Protection Plan was created directly by the Applicant or on the Applicant's behalf specifically for the RCEC. The Fire Protection Plan has economic value to the Applicant because it relates directly to the operation of the RCEC, and the Applicant has invested substantial time and resources to the creation of the Fire Protection Plan. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's operating procedures, equipment, maintenance and testing procedures, and would allow competitors to adjust their operating practices in a manner that disadvantages the Applicant.
	08-P&ID	The CEC previously granted confidential designation for "Fire Protection System Vol. 2" which contains "site-specific and detailed information" regarding

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
		RCEC's fire protection system.[13] The P&ID figures for the fire protection system contains site-specific and detailed information regarding RCEC's fire protection system and should be held confidential.
7. JOB SAFETY HAZARD ANALYSIS	Job Safety Analysis Standard	**Site Security/Vulnerability Concerns** The Job Safety Analysis Standard contains facility-specific information that discloses detailed information regarding how operational and maintenance work at the facility is assessed for hazards and threats. The Job Safety Analysis Standard also contains the non-public phone number that is used to directly contact the control room at the facility. Public disclosure of this phone number is a security concern, as that number is used for emergency and operational purposes only. **Personnel Information** The Job Safety Hazard Analysis contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The Job Safety Analysis Standard was created directly by the Applicant or on the Applicant's behalf. The Job Safety Analysis Standard has economic value to the Applicant because it relates directly to the operation of the RCEC, and the Applicant has invested substantial time and resources to the creation of the Job Safety Analysis Standard, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's operating procedures, equipment, maintenance and testing procedures, and would allow competitors to adjust their operating practices in a manner that disadvantages the Applicant.

[13] TN#: 241378, p. 9.

APPLICATION FOR CONFIDENTIAL DESIGNATION
Russell City Energy Center (01-AFC-07C)

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
	Safe Work Permit Samples	**Site Security/Vulnerability Concerns** The Safe Work Permit samples contain the non-public phone number that is used to directly contact the control room at the facility. Public disclosure of this phone number is a security concern, as that number is used for emergency and operational purposes only. The Safe Work Permits also provide information regarding risk evaluation at the RCEC site, including potential hazards associated with certain types of repairs, recommended actions, or procedures to mitigate those hazards, and information regarding repairs and maintenance work that have been performed at the facility. The Safe Work Permit Samples also identify repairs done at the facility, and methods utilized to identify and effectuate the repairs. **Personnel Information** The Safe Work Permit samples provided to CEC Staff contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy, cybersecurity, and operational security reasons. **Trade Secret/Business Information** The Safe Work Permits were developed specifically by the Applicant to ensure that OSHA requirements are met when performing work at the facility. The Safe Work Permits have economic value to the Applicant because it relates directly to maintenance activities at the RCEC, and the Applicant has invested substantial time and resources to the creation of the Safe Work Permit template, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the forms that the Applicant has developed to meet OSHA standards without the resultant expenditure of resources. This places the Applicant at a competitive disadvantage.

APPLICATION FOR CONFIDENTIAL DESIGNATION
Russell City Energy Center (01-AFC-07C)

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
8. HOT WORK PERMITS	Hot Work Permit Procedure	**Site Security/Vulnerability Concerns** The Hot Work Procedure contains the procedures for fire prevention during hot work activities at the RCEC site, including necessary clearances and fire watch durations. The Hot Work Procedure also contains file directory information from which internal operational documents can be accessed. Such information should not be publicly disclosed for privacy and cybersecurity reasons. **Personnel Information** The Hot Work Procedures contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The Job Safety Analysis Standard was created directly by the Applicant or on the Applicant's behalf. The Job Safety Analysis Standard has economic value to the Applicant because it relates directly to the operation of the RCEC, and the Applicant has invested substantial time and resources to the creation of the Job Safety Analysis Standard, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's operating procedures, equipment, maintenance and testing procedures, and would allow competitors to adjust their operating practices in a manner that disadvantages the Applicant.
	Hot Work Permits-Samples	**Site Security/Vulnerability Concerns** The Hot Work Permits samples contain the non-public phone number that is used to directly contact the control room at the facility. Public disclosure of this phone number is a security concern, as that number is used for emergency and operational purposes only.

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
		Personnel Information The Hot Work Permit samples provided to CEC Staff contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The Hot Work Permits were developed specifically by the Applicant to ensure that OSHA requirements are met when performing work at the facility. The Safe Work Permits have economic value to the Applicant because it relates directly to maintenance activities at the RCEC, and the Applicant has invested substantial time and resources to the creation of the Safe Work Permit template, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the forms that the Applicant has developed to meet OSHA standards without the resultant expenditure of resources. This places the Applicant at a competitive disadvantage.
9. CONFINED SPACE PERMITS	RCEC Combined Space Entry Standard	**Site Security/Vulnerability Concerns** The Confined Space Entry Standard contains facility-specific information that discloses detailed information regarding how operational and maintenance work at the facility is assessed for hazards and threats. The Standard identifies the facility equipment that contains entry locations, the number of entry locations. **Personnel Information** The Confined Space Entry Standard contains personnel information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The Confined Space Entry Standard was created directly by the Applicant or on the Applicant's behalf. The Confined Space Entry Standard has economic

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
		value to the Applicant because it relates directly to the operation of the RCEC, and the Applicant has invested substantial time and resources to the creation of the Confined Space Entry Standard, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's operating procedures, equipment, maintenance and testing procedures, and would allow competitors to adjust their operating practices in a manner that disadvantages the Applicant.
	Confined Space Permit Samples	**Site Security/Vulnerability Concerns** The Confined Space Permit samples contain the non-public phone number that is used to directly contact the control room at the facility. Public disclosure of this phone number is a security concern, as that number is used for emergency and operational purposes only. **Personnel Information** The Confined Space Permit samples provided to CEC Staff contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The Confined Space Permit Samples were created directly by the Applicant or on the Applicant's behalf. Although OSHA Standard 1910 provides examples of permits that can be used to meet this OSHA standard, the Confined Space Permit Samples (such as the Permit Space Reclassification Form) were created specifically by the Applicant to implement the standard as part of facility maintenance and operations. The Applicant has invested substantial time and resources to the creation of the forms. As such, the Confined Space Permits have economic value to the Applicant because it relates directly to the operation and maintenance of the RCEC. This document is not publicly available. Disclosure would

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
		cause a loss of competitive advantage as it would enable competitors to freely access the forms that the Applicant has developed to meet OSHA standards without the resultant expenditure of resources. This places the Applicant at a competitive disadvantage.
10. LOCKOUT TAGOUT PERMITS	Lockout Tagout Standard	**Site Security/Vulnerability Concerns** The Lockout Tagout ("LOTO") Standard contains facility-specific information that discloses detailed information regarding how operational and maintenance work at the facility is assessed for hazards and threats. **Personnel Information** The LOTO Standard contains personnel information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** While it is true that LOTO protocols are implemented at all industrial facilities, the LOTO Standard was created directly by the Applicant to specifically meet the requirements of OSHA Standard 1910.147 and OSHA Instruction CPL 02-00-147. Standard 1910.147 only provides the minimum performance requirements for LOTO procedures. The LOTO Standard has economic value to the Applicant because it relates directly to the operation of the RCEC, and the Applicant has invested substantial time and resources to the creation of the LOTO Standard, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's operating procedures, equipment, maintenance and testing procedures, and would allow competitors to adjust their operating practices in a manner that disadvantages the Applicant.

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
	LOTO 3068, 3069, 3070	**Site Security/Vulnerability Concerns** The Group LOTO Authorization Form not only discloses recent repairs done at the facility, but identifies which facility components are affected by the repair, The Safe Work Permits provided along with the Group LOTO Authorization forms contain the non-public phone number that is used to directly contact the control room at the facility. Public disclosure of this phone number is a security concern, as that number is used for emergency and operational purposes only. **Personnel Information** The Group LOTO Authorization Form samples and corresponding Safe Work Permits provided to CEC Staff contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The Group LOTO Authorization Form samples and corresponding Safe Work Permits were created directly by the Applicant or on the Applicant's behalf. The Applicant has invested substantial time and resources to the creation of the forms. As such, the Group LOTO Authorization Form samples and corresponding Safe Work Permits have economic value to the Applicant because it relates directly to the operation and maintenance of the RCEC. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the forms that the Applicant has developed to meet OSHA standards without the resultant expenditure of resources. This places the Applicant at a competitive disadvantage.
11. GENERATOR STEP UP MAINTENANCE DOCUMENTATION	Maintenance Plan—EDG-104 Calpine Transformer	**Site Security/Vulnerability Concerns** The Transformer Reliability Program contains detailed information regarding the transformers

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
	Reliability Program	located on the RCEC site and how operational and maintenance work for those transformers is conducted. **<u>Personnel Information</u>** The Transformer Reliability Program contains personnel information that should not be publicly disclosed for privacy and cybersecurity reasons. **<u>Trade Secret/Business Information</u>** The Transformer Reliability Program is a program created by the Applicant to not only evaluate the condition of facility transformers, but to maintain and repair the transformers to ensure safe, efficient, and reliable operation of the facility. The Transformer Reliability Program is unique to the Applicant and has economic value to the Applicant because it relates directly to the safe and reliable operation of the RCEC and helps ensure optimal performance from the facility. The Applicant has invested substantial time and resources to the creation of the Transformer Reliability Program. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's proprietary program for evaluation, maintenance, and repair of its transformers. Public disclosure of this unique program would provide competitors access to information that regarding the optimum operation and maintenance of transformers and would allow competitors to take advantage of the benefits of the Applicant's program without a similar expenditure of resources. Competitors can adjust their operating practices in a manner that disadvantages the Applicant, resulting in a competitive loss for the Applicant.

APPLICATION FOR CONFIDENTIAL DESIGNATION
Russell City Energy Center (01-AFC-07C)

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
	Annual Inspection Reports	**Site Security/Vulnerability Concerns** The Annual Inspection Reports provide detailed information regarding the condition of RCEC's transformers, necessary repairs, and contains pictures of specific components within the RCEC. This Annual Inspection Reports contain information that has been previously designated as confidential by the CEC.[14] Therefore, the Annual Inspection Reports should be similarly designated as confidential.
	Dissolved Gas in Oil Analysis Reports	**Site Security/Vulnerability Concerns** The Dissolved Gas in Oil Analysis Reports contain detailed information regarding the status of the transformers located on the RCEC site. Read together, the Reports provide information as to how the transformers are operated and their current condition. **Trade Secret/Business Information** As stated above, the Transformer Reliability Program is a program created by the Applicant to not only evaluate the condition of facility transformers, but to maintain and repair the transformers to ensure safe, efficient, and reliable operation of the facility. The Dissolved Gas in Oil Analysis Reports are an important component of this process. Information from the reports is used to determine when repairs or replacement of the transformers are required and demonstrate the overall status of the transformers. This information has economic value to the Applicant because equipment status, repairs, and replacement are all part of the costs of generation of electricity from the facility. The operational costs of a facility directly affect the costs of bids made by generating units. Public disclosure of the status of the facility's equipment and maintenance and operating procedures provides information that competitors can utilize to adjust their bids, which puts the Applicant at a competitive disadvantage as similar information regarding its competitors is not publicly available.

[14] TN#: 241378, p. 10.

APPLICATION FOR CONFIDENTIAL DESIGNATION
Russell City Energy Center (01-AFC-07C)

FOLDER TITLE	DOCUMENT DESCRIPTION	RATIONALE FOR CONFIDENTIAL DESIGNATION
12. PERSONAL PROTECTIVE EQUIPMENT	Personal Protective Equipment Standard	**Personnel Information** The PPE Standard contains personnel information, including personnel names, contact information, and other information that should not be publicly disclosed for privacy and cybersecurity reasons. **Trade Secret/Business Information** The PPE Standard was created directly by the Applicant or on the Applicant's behalf. The PPE Standard has economic value to the Applicant because it relates directly to the operation of the RCEC. The Applicant has invested substantial time and resources to the creation of the PPE Standard, which was developed specifically to meet OSHA Standards. This document is not publicly available. Disclosure would cause a loss of competitive advantage as it would enable competitors to freely access the Applicant's operating procedures, equipment, maintenance and testing procedures, and would allow competitors to adjust their operating practices in a manner that disadvantages the Applicant.

4. State whether the information may be disclosed if it is aggregated with other information or masked to conceal certain portions, and if so the degree of aggregation or masking required.

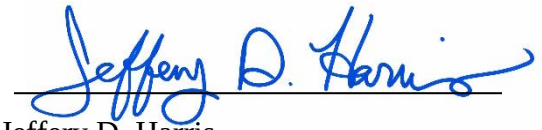
The Applicant considered whether it would be possible to aggregate or mask the information in the Site Inspection Documents. However, the Site Inspection Documents do not consist of the types of data or programmatic reporting that generally lends itself to the types of masking and aggregation the Applicant believes is contemplated by Section 2505(a)(E), thus making aggregation, or masking infeasible. However, where the CEC determines that the record can be redacted for public disclosure, the Applicant requests that the CEC consult with the Applicant to make this determination and consider instead potential production of substantially similar information.

5. State whether and how the information is kept confidential by the applicant and whether it has ever been disclosed to a person other than an employee of the applicant, and if so under what circumstances.

The Site Inspection Documents are accessible only to employees or consultants providing essential services to the Russell City Energy Center. The Site Inspection Documents have been disclosed to certain agencies, such as the California Public Utilities Commission and CEC, that have regulatory oversight or other responsibilities over either the information or the RCEC.

I certify under penalty of perjury that the information contained in this Application for Confidential Designation is true, correct, and complete to the best of my knowledge and belief. I am authorized to make this Application and Certification on behalf of the Applicants.

Dated: March 11, 2022

By: 

Jeffery D. Harris
Ellison Schneider Harris & Donlan LLP
2600 Capitol Avenue, Suite 400
Sacramento, CA 95816
Tel: (916) 447-2166
Email: jdh@eslawfirm.com

Attorneys for Russell City Energy Company, LLC