CALIFORNIA ENERGY COMMISSION
1516 NINTH STREET
SACRAMENTO, CA 95814-5512

October 30, 2008

Jeffery Harris
Ellison, Schneider & Harris LLP
2015 H Street
Sacramento, CA 95811

RE: **System Impact Study Application for Confidentiality, Ivanpah Solar Electric Generating System, Docket No. 07-AFC-5**

Dear Mr. Harris:

On September 29, 2008, Solar Partners, LLC, filed an application for confidentiality on behalf of the Ivanpah Solar Electric Generating System ("ISEGS") project (Docket No. 07-AFC-5). The application seeks confidentiality for the Interconnection System Impact Study ("SIS").

ISEGS states that the SIS:

> . . . should be held confidential indefinitely in order to protect the information identified therein. . .
>
> It has been suggested to the Applicant that the SIS may not be disclosed due to restrictions and/or prohibitions set forth in the Critical Infrastructure Information Act of 2002 ("CIIA"), codified at 6 U.S.C. §§ 131 – 134. . .related to the regulation of the use and disclosure of information submitted to the Department of Homeland Security (DHS) about vulnerabilities and threats to critical infrastructure. Further, there may be prohibitions of the use or disclosure of this information in the CAISO Tariff, including, but not necessarily limited to, Appendix U of the *California Independent System Operator Corporation FERC Electric Tarriff*. . . (the "LGIP"). In particular, the LGIP's definition of "Confidential Information" in Section 1.2.2 and the LGIP's Section 13.1 on "Confidentiality," and the subsections thereto, may include prohibitions on the use or disclosure of this information.

A properly filed application for confidentiality shall be granted under the California Code of Regulations, title 20, section 2505(a)(3)(A), "if the applicant makes a reasonable claim that the Public Records Act or other provision of law authorizes the [Energy] Commission to keep the record confidential."

Pursuant to section 131 the CIIA, The term "critical infrastructure information" means:

> information not customarily in the public domain and related to the security of critical infrastructure or protected systems -
>
> (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
>
> (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
>
> (C) 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.

Additionally, section 133 states:

> Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2) -
>
> (A) shall be exempt from disclosure under section 552 of title 5 (commonly referred to as the Freedom of Information Act);
>
> (B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;
>
> (C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any

> third party, in any civil action arising under Federal or State law if such information is submitted in good faith. . .
>
> E) shall not, if provided to a State or local government or government agency -
> (i) be made available pursuant to any State or local law requiring disclosure of information or records;
> (ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or
> (iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act. . .

ISEGS has not demonstrated that the SIS system is subject to the prohibitions in the CIIA. Specifically, ISEGS has not shown that the SIS has been submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems. Therefore, ISEGS has not made a reasonable argument under the California Energy Commission's regulations that the SIS should not be disclosed due to the restrictions of the CIIA.

ISEGS also argues that the LGIP prohibits the SIS from being disclosed. Section 1.2.2 of the LGOP defines "Confidential Information" as:

> any confidential, proprietary or trade secret information of a plan, specification, pattern, procedure, design, device, list, concept, policy or compilation relating to the present or planned business of a Party, which is designated as confidential by the Party supplying the information, whether conveyed orally, electronically, in writing, through inspection, or otherwise, subject to Section 13.1 of this LGIP.

Section 13.1 of the LGIP, titled "Confidentiality," states:

> Confidential Information shall include, without limitation, all information relating to a Party's technology, research and development, business affairs, and pricing, and any information supplied by any of the Parties to the other Parties prior to the execution of an LGIA.

However, ISEGS fails to discuss why these portions of the LGIP apply to the SIS at hand. ISEGS does not make an argument that the SIS is proprietary or trade secret information, as defined in section 1.2.2. Furthermore, ISEGS does not state that the

SIS relates to ISEGS's technology, research and development, business affairs, or pricing, pursuant to section 13.1 of the LGIP.

Therefore, ISEGS has not made a reasonable argument under the California Energy Commission's regulations that the SIS should not be disclosed due to the restrictions of the CAISO's LGIP.

Due to the reasons stated above, the application does not provide sufficient explanation upon which the Commission may grant the request, and ISEGS's application for confidential designation of the SIS is denied.

The procedures and criteria for appealing any part of this decision are set forth in the California Code of Regulations, title 20, section 2505. Be advised that an appeal of this decision must be filed within fourteen days from my decision. During those fourteen days, the SIS will not be publicly disclosed. If you have any questions concerning this matter, please contact Deborah Dyer, Senior Staff Counsel, at (916) 654-3870.

Sincerely,

Melissa Jones
Executive Director

cc: Docket Unit

Che McFarlin,
Energy Commission Project Manager