

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

<b>City of Anaheim, California</b>	)	<b>Docket No.</b>	<b>EL03-15-000</b>
	)		
<b>City of Riverside, California</b>	)	<b>Docket No.</b>	<b>EL03-20-000</b>

**ANSWER OF THE CALIFORNIA INDEPENDENT  
SYSTEM OPERATOR CORPORATION TO THE MOTION OF  
THE DEPARTMENT OF WATER RESOURCES STATE WATER  
PROJECT REGARDING THE PROTECTED STATUS OF  
CERTAIN SPECIFIED DOCUMENTS, AND MOTION FOR CONTINUED  
PROTECTION OF CERTAIN DOCUMENTS**

To: The Honorable Carmen J. Cintron  
Presiding Administrative Law Judge

Pursuant to Rule 213 of the Commission’s Rules of Practice and Procedure, 18 C.F.R. § 385.213, the California Independent System Operator Corporation (“ISO”) files this Answer to the Motion of the California Department of Water Resources State Water Project (“SWP”) for Order Confirming that the Protected Status of Certain Specified Documents and Related Testimony is Lifted (“Motion”). Although the ISO does not object to the protected status being removed from certain of the documents specified by SWP, as discussed more fully below, the ISO Tariff and a confidentiality agreement between the ISO and another entity dictate that certain documents remain protected.

**I. Basis for and Nature of SWP’s Motion**

As a threshold matter, the ISO disputes the apparent basis for SWP styling its Motion as a request for an order “confirming that the protected status ... is lifted.” The

wording of this request suggests that the conditions for removing the protection from the documents in question have been satisfied. This is not the case.

As described in the SWP Motion, under the terms of the Protective Order in this proceeding,

Any participant that contests the designation of materials as protected shall notify the party that provided the protected materials by specifying in writing the materials whose designation is contested. This Protective Order shall automatically cease to apply to such materials five (5) business days after the notification is made unless the designator, within said 5-day period, files a motion with the Presiding Administrative Law Judge, with supporting affidavits, demonstrating that the materials should continue to be protected.

Protective order at P 11.

As noted by SWP, on March 17 counsel for SWP sent counsel for the ISO a list of items for which SWP felt protected status was unwarranted. SWP included this e-mail as Attachment 1 to its Motion. In this e-mail, counsel for SWP stated "it is not evident to me that any of these materials qualify for continued protection under the APA or FERC's applicable regulations." Counsel added that "I would like to work this out with you short of asking the Judge for a ruling...." Since this e-mail was sent, there have been conversations back and forth between the parties regarding the status of the items in question.

The ISO does not believe that informal discussions, beginning with the the March 17 e-mail, constitute formal written notification pursuant to the Protective Order that the protected designation was being contested. In its Motion, however, SWP states that since the ISO has not provided the Motion supported by affidavits required by the

Protective Order, it has “waived any opportunity to seek protection for the specified documents.” Motion at 5.

The ISO strongly objects to this argument, and submits that it did not receive formal written notification that the protected status would be contested until SWP’s Motion was filed on April 27. Receiving such notification, the ISO promptly provides this pleading and the accompanying declaration of Ms. Le Vine. For this reason, the ISO cannot be viewed as having waived its rights to seek continued protection for certain of the specified documents. That being the case, SWP’s “Motion...for Order Confirming that the Protected Status ...is Lifted” must be denied.

## II. The Specified Documents

SWP disputes the protected status of the following items:

1. Operating Procedure S-326;
2. Supplemental Response to DWR-ISO-24;
3. Response to DWR-ISO-20, Attachment “DWR-ISO-20 (1<sup>st</sup> of 2).xls,” Attachment DWR-ISO-20 (2<sup>nd</sup> of 2).xls”;
4. Response to DWR-ISO-20, Attachment DWR-ISO-20B, “STS-NTS 2003.xls,” “ISO IPP Gen on STS,” and “Net ISO STS from Mona”;
5. Revised Response to CIT-ISO-22, Attachment CIT-ISO-22A.xls (Tabs: “Four Corners-Moenkopi Actual FI” and “Eldorado-Moenkopi actual flow”);
6. Response to Cities-ISO-1, Revised Cities-ISO-1A (Spreadsheet Tabs: “CIT-ISO-1,” “CIT-ISO-2,” and “CIT-ISO-3”);
7. The Transcript of the February 25, 2004 Deposition of Lonnie J. Rush in its entirety;<sup>1</sup> and

---

<sup>1</sup> SWP Item 7, the Transcript of the Deposition of Lonnie Rush, contains references to the data in SWP Item 3, for which continued protection is being sought due to the existence of a confidentiality agreement, as discussed *infra*. It also contains references to the data in SWP Item 6, for which continued protection is being sought due to the terms of the ISO Tariff. Nonetheless, as the substance of the

8. Protected excerpts of the Transcript of the March 24, 2004 Deposition of Dr. Chris Mensah-Bonsu.

Of these items, the ISO seeks continued protection for 3, 5, and 6. The ISO's for seeking this continued protection is provided below, and in the Declaration of Deborah A. Le Vine, included with this pleading as Attachment 1.

#### Items 3 and 5

Items 3 and 5 consist of discovery responses in the form of spreadsheets from the ISO's historical database. The ISO received the data for this database from the Western Electricity Coordinating Council or "WECC". The ISO is party to a Confidentiality Agreement with the WECC.<sup>2</sup> Pursuant to this agreement, the ISO may access confidential data from the WECC website. The figures in the spreadsheets referenced in SWP's Items 3 and 5 are taken from this confidential WECC data. Therefore, the ISO is not at liberty to provide this data on an unprotected basis.

If the ISO were to violate its agreement with the WECC, under Paragraph 8 of the agreement the WECC would withdraw the ISO's rights of access to the confidential data. This would undermine the ISO's ability to perform its functions as a Control Area operator, including protecting the reliability of the ISO Controlled Grid. For this reason, the ISO seeks continued protection for this document.

#### Item 6

SWP's Item 6 consists of a data response in the form of a spreadsheet. The spreadsheet includes individual bid data for which the specific Market Participant is identified by Scheduling Coordinator ID. Under Section 20.3 of the Commission-

---

Transcript's discussion of these items is such that no confidential matter is revealed, the ISO is not seeking continued protection of the Transcript itself.

<sup>2</sup> The Confidentiality Agreement is provided as Attachment 2 to this pleading.

approved ISO Tariff, the ISO is required to maintain the confidentiality of such individual bids.

Section 20.3.2 reads as follows:

The following information provided to the ISO by Scheduling Coordinators shall be treated by the ISO as confidential:

- (a) individual bids for Supplemental Energy;
- (b) individual Adjustment Bids for Congestion Management which are not designated by the Scheduling coordinator as available;
- (c) individual bids for Ancillary Services;
- (d) transactions between Scheduling Coordinators;
- (e) individual Generator Outage programs unless a Generator makes a change to its Generator Outage program which causes Congestion in the short-term (i.e. one month or less), in which case, the ISO may publish the identity of that Generator.

While there is an exception to the requirements of Section 20.3.2 for data that is more than 6 months old, since the data at issue here relates to calendar year 2003, the 6 months have yet to expire. Therefore, the requirements of the ISO Tariff require that this data remain protected.

Moreover, revealing specific bid data by customer in this manner would place Market Participants at risk of competitive disadvantage or other business injury, and thus is the precise sort of data the Protective Order is designed to protect.

**III. Conclusion**

For the reasons provided above, the ISO requests that the Presiding Administrative Law Judge deny the Motion of the SWP, and grant the ISO's Motion for continued protected treatment of Items 3, 5, and 6.

Respectfully submitted,

Charles Robinson  
General Counsel  
Anthony J. Ivancovich  
Senior Regulatory Counsel  
The California Independent  
System Operator Corporation  
151 Blue Ravine Road  
Folsom, CA 95630

/s/ Julia Moore \_\_\_\_\_  
David B. Rubin  
Michael E. Ward  
Julia Moore  
Swidler Berlin Shereff Friedman, LLP  
3000 K Street, N.W.  
Suite 300  
Washington, DC 20007

Date: May 3, 2004

# **ATTACHMENT 1**

**THE UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

City of Anaheim, California	)	Docket Nos. EL03-15
City of Riverside, California	)	EL03-20

**DECLARATION OF DEBORAH A. LE VINE REGARDING THE  
CONFIDENTIALITY OF DOCUMENTS ON BEHALF OF THE CALIFORNIA  
INDEPENDENT SYSTEM OPERATOR CORPORATION**

1. My name is Deborah A. Le Vine and I am currently employed by the California Independent System Operator (ISO) as the Director of Contracts. I have provided testimony in this proceeding previously.
2. I am providing this declaration to explain the necessity of retaining the protected status of certain documents the ISO has provided in this proceeding. The specific documents in question are the following:
  1. Response to DWR-ISO-20, Attachment "DWR-ISO-20 (1<sup>st</sup> of 2).xls;"
  2. Response to DWR-ISO-20, Attachment "DWR-ISO-20 (2<sup>nd</sup> of 2).xls;"
  3. Revised Response to CIT-ISO-22, Attachment CIT-ISO-22A.xls;
  4. Response to Cities-ISO-1, Revised Cities-ISO-1A; and

Each of these items warrant continued protected status, as I describe below.

3. The attachments to the ISO's response to DWR-ISO-20 and CIT-ISO-22 (Items 1, 2 and 3 on my list above) contain data originally derived from a Western Electricity Coordinating Council ("WECC") website to which the ISO has access through a confidentiality agreement. The purpose of this agreement is to prevent



proprietary information from being made available to entities engaged in “energy merchant functions”. Under the terms of the confidentiality agreement, the ISO is not at liberty to provide the data in question to anyone on a non-protected basis.

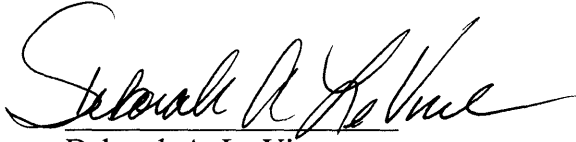
4. The ISO’s response to CIT-ISO-1 (Item 4 on the list above) contains information on bids, including specific Scheduling Coordinator IDs. Under Section 20.3 of the Commission-approved ISO Tariff, the ISO is required to maintain the confidentiality of such individual bids. Section 20.3.2 reads as follows:

The following information provided to the ISO by Scheduling Coordinators shall be treated by the ISO as confidential:

- (a) individual bids for Supplemental Energy;
- (b) individual Adjustment Bids for Congestion Management which are not designated by the Scheduling coordinator as available;
- (c) individual bids for Ancillary Services;
- (d) transactions between Scheduling Coordinators;
- (e) individual Generator Outage programs unless a Generator makes a change to its Generator Outage program which causes Congestion in the short-term (i.e. one month or less), in which case, the ISO may publish the identity of that Generator.

While there is an exception to the requirements of Section 20.3.2 for data that is more than 6 months old, since the data at issue here relates to calendar year 2003, the 6 months have yet to expire. Therefore, the requirements of the ISO Tariff require that this data remain protected.

I declare under penalty of perjury that the facts stated above are true to the best of my knowledge, information, and belief.

  
Deborah A. Le Vine

Dated the 3<sup>rd</sup> of May, 2004.

## **ATTACHMENT 2**

**Western Systems Coordinating Council  
Confidentiality Agreement for Electric System Data  
November 16, 2001**

1. **Parties to this Agreement.** This Agreement is among the Data Recipients who are the signatories to this document, and between each of the Data Recipients of the North American Electric Reliability Council (NERC) and the Western Systems Coordinating Council (WSCC).
  
2. **Background.** To maintain the operational security of the bulk electric system, the NERC and WSCC Operating Policies require that specific information, which is referred to in this Agreement as “Operational and Security Data” (Data), regarding operating conditions within each Control Area, be made available to (1) other Control Areas, (2) Security Coordinators, and (3) those entities responsible for real-time operational security. Because Operational and Security Data can be competitively sensitive in the electric energy market, and is therefore considered proprietary in nature, the availability and confidentiality of that Data must be protected. To ensure that such information is available only to those responsible for maintaining the operational security of the electricity supply in the North American power system and the Western Interconnection, and not made available nor used by any entities engaged in the Energy Merchant Functions, Operational and Security Data will be collected from all control areas and other entities who are directly responsible for the immediate, real-time operations of the bulk electric system. Such data will be made available only to those entities directly responsible for immediate real-time operational security, who are also signatories to and comply with this agreement. Any such entity is hereafter referred to as a Data Recipient.
  
3. **Definitions.**
  - 3.1. **Security Coordinator.** An entity responsible for the operational security of one or more control areas.
  
  - 3.2. **Control Area.** An electrical system bounded by interconnection (tie line) metering and telemetry. It controls its generation directly to maintain its interchange schedule with other control areas and contributes to frequency regulation of the Interconnection.
  
  - 3.3. **Operational and Security Data.** Information pertaining to the electric system which is used for analyzing the operational security of the North American power system and the Western Interconnection, including information in the EHV Data Pool and WSCCNet Message System. Security Data is available from Security Coordinators, Interregional Security Network (ISN), WSCC Operations Network (WON), control areas or other operating entities directly responsible for the immediate real-time operations of the bulk electric system.

## Confidentiality Agreement for Electric System Data

---

- 3.4. Data Supplier.** Control Areas, Security Coordinators, and other entities who are directly responsible for the immediate, real-time operations of the bulk electric system, who supply Operational and Security Data, either manually or automatically, to their Security Coordinator(s), other Security Coordinators, or other Control Areas.
- 3.5. Data Recipient.** Control Areas, Security Coordinators and other entities who are directly responsible for the immediate, real-time operations of the bulk electric system, who obtain Operational and Security Data, either manually or automatically, from their Security Coordinator(s), the WSCC WON, ISN, Control Areas or other operating entities directly responsible for the immediate real time operation of the bulk electric system.
- 3.6. WSCC Operations Network (WON).** The telecommunications and data system used to share Operational and Security Data among the Data Recipients. The WON serves as the communication medium for the WSCC EHV data pool, WSCCNet (message system) and the Inter-utility Data Exchange.
- 3.7. NERC Interregional Security Network (ISN).** The NERC communication and data system used to share Operational and Security Data among the Data Recipients.
- 3.8. Energy Merchant Function.** Any purchase or sale of electric energy or Interconnected Operations Services for any commercial reason.
- 3.9. Merchant Employee.** Within an organization, any employee who engages in Energy Merchant Functions.
- 4. Standards of Conduct.** A Data Recipient must conduct its business to conform with the following standards:

  - 4.1. General Rules.**

    - 4.1.1. Prohibitions.** Any Merchant Employee of the Data Recipient or its affiliate, engaged in Energy Merchant Functions is prohibited from having access to the Operational and Security Data, except as it may be made available to all Energy Merchant Functions simultaneously by means other than the WON or ISN.
    - 4.1.2.** Except as emergency conditions dictate as discerned by a Security Coordinator or Control Area, the employees of a Data Recipient must function independently of the Merchant Employees within that organization or its affiliates.
    - 4.1.3.** Notwithstanding any other provisions herein, in emergency circumstances that could jeopardize operational security, Data Recipients may take

## Confidentiality Agreement for Electric System Data

---

whatever steps are necessary to maintain system security. Data Recipients must report to the Security Coordinator each emergency that results in any deviation from this agreement within 12 hours of such deviation.

**4.1.4. Employee Transfers.** Employees engaged in either the Energy Merchant Function (Merchant Employees) or real-time transmission system operations reliability function are not precluded from transferring between functions as long as the transfer is not used as a means to circumvent the standards of this agreement. Notice of any employee transfer between reliability and Energy Merchant Functions shall be provided on the Open Access Same-Time Information System and to the Security Coordinator within 24 hours of the transfer.<sup>1</sup>

**4.1.5. Disclosure.** Any employee of the Data Recipient, or any employee of an affiliate, engaged in system operation reliability functions shall not disclose to Merchant Employees of the Data Recipient, or any of its affiliates, any Operational and Security Data concerning the operating conditions of the electric system based on data receive as related to this Agreement. The Data Recipient shall not, even under conditions of confidence, make available, disclose, provide, or communicate the Operational and Security Data to any other party who is not a signatory to this Agreement, to the extent law allows.

**4.1.6. Auditing.** The Data Recipient must educate its employees, and any employee of an affiliate engaged in transmission system operations, in the provisions of this Agreement and provide any information upon request to the Western Systems Coordinating Council necessary to determine compliance with the terms and conditions of this Agreement, including confidentiality agreements thereto.

**5. Disclaimer.** Each Data Recipient acknowledges and agrees that the Data Supplier generates and gathers such Operational and Security Data to meet the Supplier's sole needs and responsibilities. Each Data Supplier provides and each Data Recipient receives any and all Operational and Security Data "as is" and "with all faults, errors, defects, and inaccuracies." No Data Supplier makes any representations or warranties whatsoever with respect to the availability, currentness, accuracy, reliability, or suitability of any Operational and Security Data pursuant to this Agreement. Each Data Supplier and each Data Recipient disclaims and waives all rights and remedies that it may otherwise have with respect to any and all representations, warranties and liabilities of each Data Recipient, express or implied, arising by law or otherwise, with respect to any faults, errors, inaccuracies or omissions, availability, currentness, reliability or suitability of the Operational and Security Data. Each Data Recipient assumes any and all risk and

---

<sup>1</sup> For the purpose of this Agreement, "transfer" includes job change(s) within or between organizations such that the employee works in both functions within a six-month period.

responsibility for its selection and, or use of, and reliance on, any Operational and Security Data.

**6. Term and Termination.**

**6.1. Term.** The term of this agreement shall commence immediately upon the signature of an officer of the Data Recipient and shall remain in effect until terminated.

**6.2. Termination.** Any Data recipient wishing to terminate this agreement shall notify the WSCC in writing of its desire to terminate this agreement. Termination shall be effective 30 days following acknowledgement of receipt of such written notice, at which time the Data Recipient will be prohibited from further receipt of the Operational and Security Data.

**6.2.1.** Termination does not excuse the Data Recipient from supplying Operational and Security Data if required in NERC and WSCC Operating Policies and Criteria.

**6.2.2.** Termination does not excuse the Data Recipient from holding confidential any forecasted Operational and Security Data until eight days after the forecast period has passed.

**7. Governmental Authority.** This Agreement is subject to the laws, rules, regulations, orders and other requirements, now or hereafter in effect, of all regulatory authorities having jurisdiction over the Operational and Security Data, this Agreement, the Data Suppliers, and the Data Recipients. All laws, ordinances, rules, regulations, orders and other requirements, now or hereafter in effect, of governmental authorities that are required to be incorporated in agreements of this character are by this reference incorporated in this Agreement.

**8. Non-compliance.** Data Recipients found to be not in compliance with this Agreement by NERC or WSCC or their designated representatives will be prohibited from further receipt of the Operational and Security Data from its Security Coordinator(s), ISN, WSCC WON or Control Areas until WSCC is assured, and agrees, that the Data Recipient has resumed compliance with this Agreement. Non-compliance does not excuse the Data Recipient from supplying Operational and Security Data if required in NERC and WSCC Operating Policies and Criteria, nor does it excuse the Data Recipient from holding confidential any forecasted Operational and Security Data until the forecast period has passed.

**9. Due Diligence.** All signatories to this Agreement shall use due diligence to protect the NERC Interregional Security Network and WSCC Operations Network, as well as Operational and Security Data, from improper access.

Confidentiality Agreement for Electric System Data

---

- 10. **Disputes.** Disputes arising over issues regarding this Agreement will be settled in accordance with the dispute resolution procedures of the Western Systems Coordinating Council.
  
- 11. **Governing Law.** This Agreement shall in all respects be interpreted, construed and enforced in accordance with the laws of the state or province of the Data Recipient (without reference to rules governing conflicts of law), except to the extent such laws may be preempted by the laws of the United States of America, Canada, or Mexico as applicable.
  
- 12. **Integration.** This Agreement constitutes the entire agreement of the Parties.

OFFICER OF DATA RECIPIENT

System: \_\_\_\_\_

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

Title: \_\_\_\_\_

Date: \_\_\_\_\_



## **CERTIFICATE OF SERVICE**

I hereby certify that I have served the foregoing document upon all parties on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Folsom, CA 3<sup>rd</sup> day of May, 2004.

/s/ Sidney L. Mannheim  
Sidney L. Mannheim

**UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

<b>City of Anaheim, California</b>	)	<b>Docket No.</b>	<b>EL03-15-000</b>
	)		
<b>City of Riverside, California</b>	)	<b>Docket No.</b>	<b>EL03-20-000</b>

**ANSWER OF THE CALIFORNIA INDEPENDENT  
SYSTEM OPERATOR CORPORATION TO THE MOTION OF  
THE DEPARTMENT OF WATER RESOURCES STATE WATER  
PROJECT REGARDING THE PROTECTED STATUS OF  
CERTAIN SPECIFIED DOCUMENTS, AND MOTION FOR CONTINUED  
PROTECTION OF CERTAIN DOCUMENTS**

To: The Honorable Carmen J. Cintron  
Presiding Administrative Law Judge

Pursuant to Rule 213 of the Commission's Rules of Practice and Procedure, 18 C.F.R. § 385.213, the California Independent System Operator Corporation ("ISO") files this Answer to the Motion of the California Department of Water Resources State Water Project ("SWP") for Order Confirming that the Protected Status of Certain Specified Documents and Related Testimony is Lifted ("Motion"). Although the ISO does not object to the protected status being removed from certain of the documents specified by SWP, as discussed more fully below, the ISO Tariff and a confidentiality agreement between the ISO and another entity dictate that certain documents remain protected.

**I. Basis for and Nature of SWP's Motion**

As a threshold matter, the ISO disputes the apparent basis for SWP styling its Motion as a request for an order "confirming that the protected status ... is lifted." The

wording of this request suggests that the conditions for removing the protection from the documents in question have been satisfied. This is not the case.

As described in the SWP Motion, under the terms of the Protective Order in this proceeding,

Any participant that contests the designation of materials as protected shall notify the party that provided the protected materials by specifying in writing the materials whose designation is contested. This Protective Order shall automatically cease to apply to such materials five (5) business days after the notification is made unless the designator, within said 5-day period, files a motion with the Presiding Administrative Law Judge, with supporting affidavits, demonstrating that the materials should continue to be protected.

Protective order at P 11.

As noted by SWP, on March 17 counsel for SWP sent counsel for the ISO a list of items for which SWP felt protected status was unwarranted. SWP included this e-mail as Attachment 1 to its Motion. In this e-mail, counsel for SWP stated "it is not evident to me that any of these materials qualify for continued protection under the APA or FERC's applicable regulations." Counsel added that "I would like to work this out with you short of asking the Judge for a ruling...." Since this e-mail was sent, there have been conversations back and forth between the parties regarding the status of the items in question.

The ISO does not believe that informal discussions, beginning with the the March 17 e-mail, constitute formal written notification pursuant to the Protective Order that the protected designation was being contested. In its Motion, however, SWP states that since the ISO has not provided the Motion supported by affidavits required by the

Protective Order, it has “waived any opportunity to seek protection for the specified documents.” Motion at 5.

The ISO strongly objects to this argument, and submits that it did not receive formal written notification that the protected status would be contested until SWP’s Motion was filed on April 27. Receiving such notification, the ISO promptly provides this pleading and the accompanying declaration of Ms. Le Vine. For this reason, the ISO cannot be viewed as having waived its rights to seek continued protection for certain of the specified documents. That being the case, SWP’s “Motion...for Order Confirming that the Protected Status ...is Lifted” must be denied.

## **II. The Specified Documents**

SWP disputes the protected status of the following items:

1. Operating Procedure S-326;
2. Supplemental Response to DWR-ISO-24;
3. Response to DWR-ISO-20, Attachment “DWR-ISO-20 (1<sup>st</sup> of 2).xls,” Attachment DWR-ISO-20 (2<sup>nd</sup> of 2).xls”;
4. Response to DWR-ISO-20, Attachment DWR-ISO-20B, “STS-NTS 2003.xls,” “ISO IPP Gen on STS,” and “Net ISO STS from Mona”;
5. Revised Response to CIT-ISO-22, Attachment CIT-ISO-22A.xls (Tabs: “Four Corners-Moenkopi Actual FI” and “Eldorado-Moenkopi actual flow”);
6. Response to Cities-ISO-1, Revised Cities-ISO-1A (Spreadsheet Tabs: “CIT-ISO-1,” “CIT-ISO-2,” and “CIT-ISO-3”);
7. The Transcript of the February 25, 2004 Deposition of Lonnie J. Rush in its entirety;<sup>1</sup> and

---

<sup>1</sup> SWP Item 7, the Transcript of the Deposition of Lonnie Rush, contains references to the data in SWP Item 3, for which continued protection is being sought due to the existence of a confidentiality agreement, as discussed *infra*. It also contains references to the data in SWP Item 6, for which continued protection is being sought due to the terms of the ISO Tariff. Nonetheless, as the substance of the

8. Protected excerpts of the Transcript of the March 24, 2004 Deposition of Dr. Chris Mensah-Bonsu.

Of these items, the ISO seeks continued protection for 3, 5, and 6. The ISO's for seeking this continued protection is provided below, and in the Declaration of Deborah A. Le Vine, included with this pleading as Attachment 1.

#### Items 3 and 5

Items 3 and 5 consist of discovery responses in the form of spreadsheets from the ISO's historical database. The ISO received the data for this database from the Western Electricity Coordinating Council or "WECC". The ISO is party to a Confidentiality Agreement with the WECC.<sup>2</sup> Pursuant to this agreement, the ISO may access confidential data from the WECC website. The figures in the spreadsheets referenced in SWP's Items 3 and 5 are taken from this confidential WECC data. Therefore, the ISO is not at liberty to provide this data on an unprotected basis.

If the ISO were to violate its agreement with the WECC, under Paragraph 8 of the agreement the WECC would withdraw the ISO's rights of access to the confidential data. This would undermine the ISO's ability to perform its functions as a Control Area operator, including protecting the reliability of the ISO Controlled Grid. For this reason, the ISO seeks continued protection for this document.

#### Item 6

SWP's Item 6 consists of a data response in the form of a spreadsheet. The spreadsheet includes individual bid data for which the specific Market Participant is identified by Scheduling Coordinator ID. Under Section 20.3 of the Commission-

---

Transcript's discussion of these items is such that no confidential matter is revealed, the ISO is not seeking continued protection of the Transcript itself.

<sup>2</sup> The Confidentiality Agreement is provided as Attachment 2 to this pleading.

approved ISO Tariff, the ISO is required to maintain the confidentiality of such individual bids.

Section 20.3.2 reads as follows:

The following information provided to the ISO by Scheduling Coordinators shall be treated by the ISO as confidential:

- (a) individual bids for Supplemental Energy;
- (b) individual Adjustment Bids for Congestion Management which are not designated by the Scheduling coordinator as available;
- (c) individual bids for Ancillary Services;
- (d) transactions between Scheduling Coordinators;
- (e) individual Generator Outage programs unless a Generator makes a change to its Generator Outage program which causes Congestion in the short-term (i.e. one month or less), in which case, the ISO may publish the identity of that Generator.

While there is an exception to the requirements of Section 20.3.2 for data that is more than 6 months old, since the data at issue here relates to calendar year 2003, the 6 months have yet to expire. Therefore, the requirements of the ISO Tariff require that this data remain protected.

Moreover, revealing specific bid data by customer in this manner would place Market Participants at risk of competitive disadvantage or other business injury, and thus is the precise sort of data the Protective Order is designed to protect.

### III. Conclusion

For the reasons provided above, the ISO requests that the Presiding Administrative Law Judge deny the Motion of the SWP, and grant the ISO's Motion for continued protected treatment of Items 3, 5, and 6.

Respectfully submitted,

Charles Robinson  
General Counsel  
Anthony J. Ivancovich  
Senior Regulatory Counsel  
The California Independent  
System Operator Corporation  
151 Blue Ravine Road  
Folsom, CA 95630

/s/ Julia Moore  
David B. Rubin  
Michael E. Ward  
Julia Moore  
Swidler Berlin Shereff Friedman, LLP  
3000 K Street, N.W.  
Suite 300  
Washington, DC 20007

Date: May 3, 2004

# **ATTACHMENT 1**



**THE UNITED STATES OF AMERICA  
BEFORE THE  
FEDERAL ENERGY REGULATORY COMMISSION**

City of Anaheim, California	)	Docket Nos. EL03-15
City of Riverside, California	)	EL03-20

**DECLARATION OF DEBORAH A. LE VINE REGARDING THE  
CONFIDENTIALITY OF DOCUMENTS ON BEHALF OF THE CALIFORNIA  
INDEPENDENT SYSTEM OPERATOR CORPORATION**

1. My name is Deborah A. Le Vine and I am currently employed by the California Independent System Operator (ISO) as the Director of Contracts. I have provided testimony in this proceeding previously.
2. I am providing this declaration to explain the necessity of retaining the protected status of certain documents the ISO has provided in this proceeding. The specific documents in question are the following:
  1. Response to DWR-ISO-20, Attachment “DWR-ISO-20 (1<sup>st</sup> of 2).xls;”
  2. Response to DWR-ISO-20, Attachment “DWR-ISO-20 (2<sup>nd</sup> of 2).xls;”
  3. Revised Response to CIT-ISO-22, Attachment CIT-ISO-22A.xls;
  4. Response to Cities-ISO-1, Revised Cities-ISO-1A; andEach of these items warrant continued protected status, as I describe below.
3. The attachments to the ISO’s response to DWR-ISO-20 and CIT-ISO-22 (Items 1, 2 and 3 on my list above) contain data originally derived from a Western Electricity Coordinating Council (“WECC”) website to which the ISO has access through a confidentiality agreement. The purpose of this agreement is to prevent

proprietary information from being made available to entities engaged in “energy merchant functions”. Under the terms of the confidentiality agreement, the ISO is not at liberty to provide the data in question to anyone on a non-protected basis.

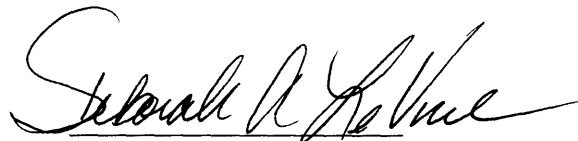
4. The ISO’s response to CIT-ISO-1 (Item 4 on the list above) contains information on bids, including specific Scheduling Coordinator IDs. Under Section 20.3 of the Commission-approved ISO Tariff, the ISO is required to maintain the confidentiality of such individual bids. Section 20.3.2 reads as follows:

The following information provided to the ISO by Scheduling Coordinators shall be treated by the ISO as confidential:

- (a) individual bids for Supplemental Energy;
- (b) individual Adjustment Bids for Congestion Management which are not designated by the Scheduling coordinator as available;
- (c) individual bids for Ancillary Services;
- (d) transactions between Scheduling Coordinators;
- (e) individual Generator Outage programs unless a Generator makes a change to its Generator Outage program which causes Congestion in the short-term (i.e. one month or less), in which case, the ISO may publish the identity of that Generator.

While there is an exception to the requirements of Section 20.3.2 for data that is more than 6 months old, since the data at issue here relates to calendar year 2003, the 6 months have yet to expire. Therefore, the requirements of the ISO Tariff require that this data remain protected.

I declare under penalty of perjury that the facts stated above are true to the best of my knowledge, information, and belief.

  
Deborah A. Le Vine

Dated the 3<sup>rd</sup> of May, 2004.

## **ATTACHMENT 2**

**Western Systems Coordinating Council  
Confidentiality Agreement for Electric System Data  
November 16, 2001**

1. **Parties to this Agreement.** This Agreement is among the Data Recipients who are the signatories to this document, and between each of the Data Recipients of the North American Electric Reliability Council (NERC) and the Western Systems Coordinating Council (WSCC).
  
2. **Background.** To maintain the operational security of the bulk electric system, the NERC and WSCC Operating Policies require that specific information, which is referred to in this Agreement as “Operational and Security Data” (Data), regarding operating conditions within each Control Area, be made available to (1) other Control Areas, (2) Security Coordinators, and (3) those entities responsible for real-time operational security. Because Operational and Security Data can be competitively sensitive in the electric energy market, and is therefore considered proprietary in nature, the availability and confidentiality of that Data must be protected. To ensure that such information is available only to those responsible for maintaining the operational security of the electricity supply in the North American power system and the Western Interconnection, and not made available nor used by any entities engaged in the Energy Merchant Functions, Operational and Security Data will be collected from all control areas and other entities who are directly responsible for the immediate, real-time operations of the bulk electric system. Such data will be made available only to those entities directly responsible for immediate real-time operational security, who are also signatories to and comply with this agreement. Any such entity is hereafter referred to as a Data Recipient.
  
3. **Definitions.**
  - 3.1. **Security Coordinator.** An entity responsible for the operational security of one or more control areas.
  
  - 3.2. **Control Area.** An electrical system bounded by interconnection (tie line) metering and telemetry. It controls its generation directly to maintain its interchange schedule with other control areas and contributes to frequency regulation of the Interconnection.
  
  - 3.3. **Operational and Security Data.** Information pertaining to the electric system which is used for analyzing the operational security of the North American power system and the Western Interconnection, including information in the EHV Data Pool and WSCCNet Message System. Security Data is available from Security Coordinators, Interregional Security Network (ISN), WSCC Operations Network (WON), control areas or other operating entities directly responsible for the immediate real-time operations of the bulk electric system.

## Confidentiality Agreement for Electric System Data

---

- 3.4. Data Supplier.** Control Areas, Security Coordinators, and other entities who are directly responsible for the immediate, real-time operations of the bulk electric system, who supply Operational and Security Data, either manually or automatically, to their Security Coordinator(s), other Security Coordinators, or other Control Areas.
- 3.5. Data Recipient.** Control Areas, Security Coordinators and other entities who are directly responsible for the immediate, real-time operations of the bulk electric system, who obtain Operational and Security Data, either manually or automatically, from their Security Coordinator(s), the WSCC WON, ISN, Control Areas or other operating entities directly responsible for the immediate real time operation of the bulk electric system.
- 3.6. WSCC Operations Network (WON).** The telecommunications and data system used to share Operational and Security Data among the Data Recipients. The WON serves as the communication medium for the WSCC EHV data pool, WSCCNet (message system) and the Inter-utility Data Exchange.
- 3.7. NERC Interregional Security Network (ISN).** The NERC communication and data system used to share Operational and Security Data among the Data Recipients.
- 3.8. Energy Merchant Function.** Any purchase or sale of electric energy or Interconnected Operations Services for any commercial reason.
- 3.9. Merchant Employee.** Within an organization, any employee who engages in Energy Merchant Functions.
- 4. Standards of Conduct.** A Data Recipient must conduct its business to conform with the following standards:

  - 4.1. General Rules.**

    - 4.1.1. Prohibitions.** Any Merchant Employee of the Data Recipient or its affiliate, engaged in Energy Merchant Functions is prohibited from having access to the Operational and Security Data, except as it may be made available to all Energy Merchant Functions simultaneously by means other than the WON or ISN.
    - 4.1.2.** Except as emergency conditions dictate as discerned by a Security Coordinator or Control Area, the employees of a Data Recipient must function independently of the Merchant Employees within that organization or its affiliates.
    - 4.1.3.** Notwithstanding any other provisions herein, in emergency circumstances that could jeopardize operational security, Data Recipients may take

whatever steps are necessary to maintain system security. Data Recipients must report to the Security Coordinator each emergency that results in any deviation from this agreement within 12 hours of such deviation.

**4.1.4. Employee Transfers.** Employees engaged in either the Energy Merchant Function (Merchant Employees) or real-time transmission system operations reliability function are not precluded from transferring between functions as long as the transfer is not used as a means to circumvent the standards of this agreement. Notice of any employee transfer between reliability and Energy Merchant Functions shall be provided on the Open Access Same-Time Information System and to the Security Coordinator within 24 hours of the transfer.<sup>1</sup>

**4.1.5. Disclosure.** Any employee of the Data Recipient, or any employee of an affiliate, engaged in system operation reliability functions shall not disclose to Merchant Employees of the Data Recipient, or any of its affiliates, any Operational and Security Data concerning the operating conditions of the electric system based on data receive as related to this Agreement. The Data Recipient shall not, even under conditions of confidence, make available, disclose, provide, or communicate the Operational and Security Data to any other party who is not a signatory to this Agreement, to the extent law allows.

**4.1.6. Auditing.** The Data Recipient must educate its employees, and any employee of an affiliate engaged in transmission system operations, in the provisions of this Agreement and provide any information upon request to the Western Systems Coordinating Council necessary to determine compliance with the terms and conditions of this Agreement, including confidentiality agreements thereto.

**5. Disclaimer.** Each Data Recipient acknowledges and agrees that the Data Supplier generates and gathers such Operational and Security Data to meet the Supplier's sole needs and responsibilities. Each Data Supplier provides and each Data Recipient receives any and all Operational and Security Data "as is" and "with all faults, errors, defects, and inaccuracies." No Data Supplier makes any representations or warranties whatsoever with respect to the availability, currentness, accuracy, reliability, or suitability of any Operational and Security Data pursuant to this Agreement. Each Data Supplier and each Data Recipient disclaims and waives all rights and remedies that it may otherwise have with respect to any and all representations, warranties and liabilities of each Data Recipient, express or implied, arising by law or otherwise, with respect to any faults, errors, inaccuracies or omissions, availability, currentness, reliability or suitability of the Operational and Security Data. Each Data Recipient assumes any and all risk and

---

<sup>1</sup> For the purpose of this Agreement, "transfer" includes job change(s) within or between organizations such that the employee works in both functions within a six-month period.

## Confidentiality Agreement for Electric System Data

---

responsibility for its selection and, or use of, and reliance on, any Operational and Security Data.

### **6. Term and Termination.**

**6.1. Term.** The term of this agreement shall commence immediately upon the signature of an officer of the Data Recipient and shall remain in effect until terminated.

**6.2. Termination.** Any Data recipient wishing to terminate this agreement shall notify the WSCC in writing of its desire to terminate this agreement. Termination shall be effective 30 days following acknowledgement of receipt of such written notice, at which time the Data Recipient will be prohibited from further receipt of the Operational and Security Data.

**6.2.1.** Termination does not excuse the Data Recipient from supplying Operational and Security Data if required in NERC and WSCC Operating Policies and Criteria.

**6.2.2.** Termination does not excuse the Data Recipient from holding confidential any forecasted Operational and Security Data until eight days after the forecast period has passed.

**7. Governmental Authority.** This Agreement is subject to the laws, rules, regulations, orders and other requirements, now or hereafter in effect, of all regulatory authorities having jurisdiction over the Operational and Security Data, this Agreement, the Data Suppliers, and the Data Recipients. All laws, ordinances, rules, regulations, orders and other requirements, now or hereafter in effect, of governmental authorities that are required to be incorporated in agreements of this character are by this reference incorporated in this Agreement.

**8. Non-compliance.** Data Recipients found to be not in compliance with this Agreement by NERC or WSCC or their designated representatives will be prohibited from further receipt of the Operational and Security Data from its Security Coordinator(s), ISN, WSCC WON or Control Areas until WSCC is assured, and agrees, that the Data Recipient has resumed compliance with this Agreement. Non-compliance does not excuse the Data Recipient from supplying Operational and Security Data if required in NERC and WSCC Operating Policies and Criteria, nor does it excuse the Data Recipient from holding confidential any forecasted Operational and Security Data until the forecast period has passed.

**9. Due Diligence.** All signatories to this Agreement shall use due diligence to protect the NERC Interregional Security Network and WSCC Operations Network, as well as Operational and Security Data, from improper access.



Confidentiality Agreement for Electric System Data

---

10. **Disputes.** Disputes arising over issues regarding this Agreement will be settled in accordance with the dispute resolution procedures of the Western Systems Coordinating Council.
11. **Governing Law.** This Agreement shall in all respects be interpreted, construed and enforced in accordance with the laws of the state or province of the Data Recipient (without reference to rules governing conflicts of law), except to the extent such laws may be preempted by the laws of the United States of America, Canada, or Mexico as applicable.
12. **Integration.** This Agreement constitutes the entire agreement of the Parties.

OFFICER OF DATA RECIPIENT

System: \_\_\_\_\_

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

Title: \_\_\_\_\_

Date: \_\_\_\_\_

**CERTIFICATE OF SERVICE**

I hereby certify that I have served the foregoing document upon all parties on the official service list compiled by the Secretary in the above-captioned proceeding, in accordance with the requirements of Rule 2010 of the Commission's Rules of Practice and Procedure (18 C.F.R. § 385.2010).

Dated at Folsom, CA 3<sup>rd</sup> day of May, 2004.

/s/ Sidney L. Mannheim  
Sidney L. Mannheim