California ISO
Your Link to Power

California Independent
System Operator Corporation

Memorandum

To: ISO Board of Governors

From: Nancy Saracino, Chief Compliance Officer

Date: July 1, 2008

Re: **Compliance Committee Update**

This memorandum does not require Board action.

This provides the second report of the Compliance Committee with respect to compliance efforts this year.

<u>Implementation</u>

Implementation of the Compliance Program has been ongoing since its approval by the Board in 2007, and will continue at least through 2008.

Reliability Standards Compliance

Due to the need to report on confidential matters, the report on the mandatory reliability standards is contained in the Board's executive session materials.

Tariff Compliance

The Compliance Committee is also developing a proposed tariff compliance program utilizing a structure similar the structure of the Reliability Standards Compliance program. The program will require each Business Unit to identify a compliance "coordinator". This individual would be responsible for mapping each tariff responsibility of that Business Unit to a specific job. The results should be documented in individual Pay for Performance Plans and in the Business Units' business processes. The legal department is in the process of identifying attorneys and paralegals to assist compliance coordinators in identifying a responsible Business Unit for each tariff obligation. In addition, the Business Units and compliance coordinators will be responsible for developing tailored compliance programs, including training and any additional procedures to ensure compliance. The assigned attorneys will also provide guidance and review draft materials to ensure consistency with the tariff and any manuals and procedures that implement the tariff. The proposed program will be explained to employees during the annual mandatory compliance training.

Substance Abuse Prevention Policy

The Compliance Committee coordinated the development and implementation of a new corporate policy, the Substance Abuse Prevention Policy, which replaces the existing Fitness for Duty Policy. This new policy is effective July 1, 2008, and will be the subject of specific training as described below. Essentially, the new policy carries forward the restrictions contained in the prior policy and provides significant additional clarity in this important area. Specifically, the new policy addresses definitional issues, what constitutes prohibited conduct, what disciplinary action may be taken, and describes drug testing procedures, with a focus on awareness and prevention supported by the employee assistance program.

Training

Mandatory Critical Infrastructure Protection Standards Training

NERC Critical Infrastructure Protection (CIP) Standard 002-009 mandates the California ISO to implement and maintain a cyber security program and to protect cyber assets critical to reliable bulk electric system operation. NERC CIP-004 requires mandatory security training for all individuals having authorized cyber or authorized unescorted physical access to critical assets within 90 days of access being granted and annually there after. Critical assets include facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system.

CAISO completed this year's mandatory annual training for all employees with access to Critical Assets as of June 30. Employees that do not have access to critical assets will also take security training as an adjunct to the *Employee Mandatory Training* program below.

Employee Mandatory Training

This year's mandatory training for all employees is currently underway and is expected to be completed by the end of August. The mandatory training for all employees includes the following subjects: (i) the Employees Code of Conduct and Ethical Principles; (ii) Mandatory Standards Compliance; (iii) Tariff Compliance; (iv) Workplace Safety; (v) the Emergency Management Program; (vi) the Substance Abuse Prevention Policy; and (vii) Information and Physical Security.

Coordination and Next Steps

The Compliance Committee continues to coordinate with all compliance-related functions within the organization to fill gaps, avoid duplication, and maximize the value of our efforts to continuously improve compliance monitoring and reporting with the resources we have available. Clearly, compliance related activities will continue to require a significant commitment of time and resources, and the Compliance Committee will continue its efforts to provide regular reports to apprise the Board of its activities during this important implementation period.