California ISO
Shaping a Renewed Future

California Independent System Operator Corporation

Memorandum

To: Audit Committee of the ISO Board of Governors

From: Roger Collanton, Vice President, General Counsel & Chief Compliance Officer

Date: March 12, 2014

Re: **Compliance update**

This memorandum does not require Committee action.

The Board of Governors' *Compliance and Ethics Program Policy* provides that the Chief Compliance Officer will administer the ISO's compliance and ethics program "under the oversight of the Audit Committee of the Board of Governors," and with support from Executive Management and the Compliance and Ethics Committee. The Compliance and Ethics Committee met on January 14, 2014, to discuss compliance goals for 2014, and code of conduct compliance, among other things. This is the Chief Compliance Officer's update on significant compliance initiatives since the previous report, dated December 11, 2013.

Updated compliance risk assessment and compliance monitoring

In 2011, the Corporate Compliance group worked with an outside expert to identify, rate and prioritize compliance risks. Based on individual interviews and focus groups covering a cross-section of ISO business units, the team produced a report that prioritized compliance risks in all areas including NERC mandatory standards, corporate policies, the tariff and other FERC regulatory requirements.

In late 2013, the Corporate Compliance group updated that assessment, to reflect changes since the 2011 report. The update identifies new areas of compliance risk and the steps the ISO is taking to mitigate those risks. It also identifies new steps the ISO is taking to mitigate risks that were identified in the original 2011 report. This updated risk assessment became the basis for the 2013-14 compliance monitoring program. This program involves monitoring the compliance risks identified in the assessment, either on an ongoing or scheduled basis as appropriate for each risk, with a focus on the adequacy of the ISO's controls.

Compliance automation system

As part of a project to automate the processes through which the ISO documents compliance with NERC's mandatory reliability standards, the ISO purchased a software package known as a "governance, risk-management and compliance tool." The technology division has been working to configure the software for the ISO's business units. One part is scheduled to go live at the end of March – specifically, automating the management of operating procedures. The software will automatically create a separate audit trail for each part of an operating procedure, as opposed to tracking changes to a document as a whole, which will improve Operations' ability to quickly learn the history of any particular provision.

The project is on track to implement the remaining aspects of the software by the third quarter of this year. When implemented, the software will allow the ISO to:

- Review data relevant to compliance instantaneously in a dashboard format;
- Monitor compliance more efficiently, by continually gathering and maintaining the relevant evidence;
- Automate management of compliance assessments; and
- Facilitate internal reviews and external audits based on NERC's forthcoming risk-based approach to compliance (summarized below).

Risk-based controls

In 2015, NERC will begin to change its enforcement process and its evidentiary requirements to place greater emphasis on standards that are deemed more important for reliability. In addition, NERC will change the focus of its audits to emphasize the tools and processes that a utility applies to assure compliance, as opposed to simply evidence of compliance. The ISO is working to recalibrate its compliance framework accordingly.

To accomplish this transition, the project team has been developing an internal framework for assessing risk, identifying, developing and evaluating controls, and identifying evidence of compliance that will be consistent with NERC's new expectations. Phase I of the project involved seventeen of NERC's seventy reliability standards, including all eight of the critical infrastructure protection standards, three planning standards, and six operational standards. The team completed Phase I in 2013.

Phase II involves 28 additional standards, mostly related to operations and planning. It will also cover forthcoming changes to the standards about critical infrastructure protection. Although those changes will not become effective until 2016, the team is addressing them now due to the potential lead time that may be necessary for IT changes.

The project schedule calls for the team to address all seventy standards by the end of 2015.