California ISO

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 17, 2016

Re: Compliance Committee 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 December 16, 2015. This is the Chief Compliance Officer's update on significant compliance initiatives since the previous report, dated December 10, 2015.

NERC risk-based controls

Effective in 2015, NERC changed its enforcement process and evidentiary requirements to place greater emphasis on mandatory reliability standards that are deemed more important for maintaining system reliability. In addition, NERC modified its audits to focus on risk-based controls, meaning the tools and processes that a utility applies to assure compliance with standard, as opposed to evidence of compliance.

The ISO has been working since 2013 to recalibrate its compliance framework in response to these NERC changes. The final phase of this project is planned for 2016.

The project team initially developed an internal framework for assessing risk, identifying, developing and evaluating controls, and identifying evidence of compliance to be consistent with NERC's new expectations. Phase I of the project implemented this framework for 17 of the 70 reliability standards. Phase II covered 28 additional standards, mostly related to operations and planning, as well as forthcoming changes to the critical infrastructure protection standards. These two phases were completed in 2013 and 2014 in preparation for WECC's tri-annual audit in 2015.

In 2016, the project team is scheduled to complete the project by implementing the framework for the remaining standards that were deemed lower risk. When completed and approved, the work will be imported into CENTRIC – a software package the ISO implemented in 2014 that allows ISO personnel 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 new risk-based approach to compliance (which is summarized above).

Implementation of CIP versions 5 and 6

The effective date for version 5 of the critical infrastructure protection (CIP) cybersecurity standards has been scheduled for April 1, 2016, though FERC recently postponed it by three months until July 1. The ISO embraced the transition to version 5 early and submitted its evidence to WECC during the audit last fall. The WECC auditors had no compliance findings for CIP version 5, but identified six areas of concern and made one recommendation, all around documentation. The ISO has addressed the issues raised by WECC, and management has decided to proceed with implementation by April 1, ahead of the new deadline.

FERC recently approved CIP version 6 standards effective starting July 1. Information Security is planning to track to CIP version 6 compliance by the internal target date of April 1.