Memorandum

To: Audit Committee of the ISO Board of Governors

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

Date: July 8, 2014

Re: **Compliance Committee update**

This memorandum does not require Committee action.

The *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 May 15, 2014, to review compliance responsibilities and the role of the Committee, among other matters. This is the Chief Compliance Officer's update on significant compliance initiatives.

Records management

The records management program team has begun to apply records retention requirements to systems and applications in which the ISO stores large volumes of data. These efforts involve work with the information technology division to understand the systems and data, and also with the legal group to ensure compliance with FERC requirements. The team has also initiated outreach to other ISOs and RTOs to understand their similar efforts and discuss best practices.

In addition, the team has continued efforts to identify and process records with expired retention periods, both in paper and electronic form, including those in offsite storage. The team is also working to deliver new tools and training to help employees reduce the growing volume of email.

Reliability Standards Agreements

The ISO is party to several "Reliability Standards Agreements," with its participating transmission owners which allocate responsibility for compliance with certain mandatory reliability standards relating to the transmission operator function between the ISO and the transmission owners. The ISO's Corporate Compliance and Legal departments have been working with the transmission owners to revise these agreements to assign responsibility more clearly in light of accumulated

experience with the standards and regulatory enforcement. This significant undertaking, which began in 2012, is ongoing and is anticipated to be completed by the end of this year.

Compliance training

In June, contractors who work on site and all employees completed the mandatory computer-based training about information security and protecting critical infrastructure. This training satisfies NERC mandatory standards for critical infrastructure protection. The only exceptions were personnel who are on leave of absence; they will be required to complete training when they return before their access is reinstated.