Memorandum

To: Audit Committee of the ISO Board of Governors

From: Nancy Saracino, Chief Compliance Officer

Date: March 13, 2013

Re: **Compliance Update**

This memorandum does not require Committee action.

The *Compliance and Ethics Program Policy* provides that the Chief Compliance Officer administer the ISO's compliance 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. This is the report of the Chief Compliance Officer and the Compliance and Ethics Committee about progress on significant compliance initiatives since the last report on December 6, 2012.

The Compliance and Ethics Committee met on December 17, 2012 and February 19, 2013. A status report on major compliance initiatives follows.

Records Management

In January 2013, the ISO rolled out a new records retention schedule to all employees. Over the next year, we will be working toward achieving compliance with that schedule. The first area of focus has been electronic records. To encourage deletion of old e-mails consistent with the records retention policy and the new schedule, the ISO implemented a 5 GB limit on employee mailboxes effective March 1. This was a large effort across the company, and by the effective date the ISO had 100% compliance. This was successful because each employee devoted time and attention to this project. The records management program will continue with a number of initiatives throughout the year.

Compliance Automation and Risk-Based Controls

The ISO has begun a project to automate the processes through which the ISO documents compliance with NERC's mandatory reliability standards. Currently, during a self-certification period or audit, compliance personnel must reach out to the affected operational employees to gather evidence of compliance. The project will automate this process by developing a system that triggers requests for evidence of compliance at the appropriate times, requests approvals from the relevant managers, and retains the evidence. Once the system is developed, the ISO expects to apply it to other compliance requirements, including audits of its bid-to-bill processes and controls on tariff compliance.

The project team is also working to build on the compliance automation system by tracking NERC's forthcoming change to focus on standards according to the risk presented. Although NERC does not currently prioritize among the various mandatory reliability standards – it gives them all equal weight – that will change beginning in 2015. At that time, NERC will begin to place greater emphasis on standards that it considers to present greater reliability risk. The ISO's project will align with the developments at NERC so that the ISO's automated compliance system will reflect the same priorities and tiers of standards when those priorities become effective. This will enable the ISO to readily demonstrate its risk-based compliance methodology as being in alignment with the new NERC forward-looking audit practices. It will also enable an increased focus on those standards judged as higher risk, while simultaneously ensuring across-the-board compliance with all mandatory standards.

Data Regarding Employee Access to Critical Cyber Assets

To ensure that the ISO can promptly produce accurate reports about employee access to critical cyber assets, and to satisfy the related NERC standard (CIP-004), the Human Resources and Technology divisions completed a project in February to revise the associated processes and systems. The project included both extensive validation of the source data and automating the process for producing reports from that data. As a result, full reports about all employees can now be generated on demand, whereas the report generation previously took several days. This makes it easier to validate the ISO's compliance on a regular basis.

Information Security

The Technology division has begun work on a project to enhance the ISO's information security by pursuing a number of discrete projects based on recommendations made by a consultant in 2012. When completed, the projects will improve the ISO's standing with respect to recognized standards for information security systems (the ISO 27000 series). The projects include bolstering business processes, upgrading systems and improving the use of current systems.