

February 16th 2005

ISO/RTO Council General comments to NERC CIP Draft Standards 002-009

The standard still looks inconsistent in a number of areas:

- a) Some of the measures and requirements language seems to be similar both in the same section of the standards and across the standards.
- b) The numbering is still inconsistent.
- c) It is clear that a professional technical writer has not looked at these standards to make it clear and homogenous.

These inconsistencies have caused much time to be wasted by review teams which is regrettable considering it could have been easily solved.

The time periods prescribed throughout are still inconsistent across the CIP 002 to 009 standards.

If an entity is found not to have properly identified its critical infrastructure in 002, will this mean being scored as non-compliant in the other remaining standards?

The standard does not clearly require a security and governance program if it is determined that there are no critical assets. The standards must require that a program exists regardless of whether critical assets exist. The standard should state that the entity must perform an annual review to reconfirm its position on cyber assets. As such, the order of 002 and 003 should be reversed.

Most references to unattended facilities do not seem to bear relevance on security measures to critical cyber assets and should be reviewed.

NERC needs to ensure that the level of non-compliance is commensurate to the violation's impact to reliability rather than merely being an administrative violation.