NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

Implementation Plan

Second Renewal of Urgent Action Cyber Security Standard

June 1, 2005

The purpose of NERC's cyber security standards is to ensure that all entities responsible for the reliability of the bulk electric systems of North America identify and protect critical cyber assets that control or could impact the reliability of the bulk electric systems. An urgent action cyber security standard was initially adopted in August 2003 and renewed for a second year in August 2004. A permanent cyber security standard has been under development and is expected to be submitted to ballot later in 2005. The Urgent Action Cyber Security Standard will be balloted in July 2005 for a second one-year extension beginning August 13, 2005, to allow sufficient time for the completion of the proposed permanent standard.

This implementation plan is a continuation and update of the implementation plan used for the urgent action cyber security standard since August 2003. This updated implementation plan is intended to become effective August 13, 2005 and remain in effect until August 13, 2006, or the effective date of the permanent standard, whichever is sooner.

The major difference in the implementation of this second renewal compared to the prior two years is that control areas will be replaced by balancing authorities and transmission operators, to be consistent with the adoption of the new reliability standards and the functional registration effective April 1, 2005. The NERC Compliance and Enforcement Program (CEP) will therefore evaluate only balancing authorities, transmission operators, and reliability coordinators for compliance with this standard. Some entities registered as balancing authorities and transmission operators were not previously identified as control areas and therefore did not have to self-certify for compliance with this standard. To ensure a smooth transition for the renewal, only those balancing authorities and transmission operators who were previously monitored for compliance as control areas are required to self-certify during the new extension period. Other entities identified in the standard are expected to work to meet the requirements of the standard; however, self-certification forms will not be required.

Compliance with this standard will be evaluated in the first quarter of 2006, as an update to the self-certifications completed in the first quarters of 2004 and 2005. NERC and its regions will continue to monitor compliance through the use of self-certification forms. The regions will distribute these forms to the balancing authorities, transmission operators, and reliability coordinators within their respective regions. Regions may ask other entities to provide self-certify if the region believes that these entities are performing one of the functions identified in the standard. In such cases, the completion of a self-certification form by those other than balancing authorities, transmission operators, and reliability coordinators will be at the entity’s discretion.

All balancing authorities, transmission operators, and reliability coordinators will complete and submit the appropriate regional self-certification renewal form(s) during the first quarter of 2006, indicating their compliance or degree of non-compliance with the requirements of the cyber security standard. These self-certification forms will be submitted to the appropriate NERC regional reliability council, which will hold the individual responses in confidence.

Compliance with the standard will be used to determine the overall level of cyber security preparedness in the industry. Self-certification results will be aggregated by the regions and reported to NERC. This data will illustrate whether the industry is substantially compliant with the standard in the beginning of 2006. Neither the regions nor NERC will issue letters of non-compliance to those who indicate, via self-certification, that they do not fully comply with the requirements of this standard. Neither the regions nor NERC will conduct audits to verify the self-certifications. No monetary sanctions will be levied for violations of this standard.

This implementation plan will terminate when it expires or when it is replaced by the adoption of a permanent cyber security standard implementation plan.