NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

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

June 2, 2004

Implementation Plan — Renewal of Urgent Action Cyber Security Standard

This implementation plan is a continuation and update of the implementation plan for the Urgent Action Cyber Security Standard approved in 2003. This implementation plan is intended to be in effect for the anticipated extension of the urgent action standard.

The Urgent Action Cyber Security Standard will be balloted in July for a one-year extension beginning August 13, 2004, to allow sufficient time for development of a permanent standard.

The intent of the proposed NERC cyber security standard 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.

Although the urgent action cyber security standard is written using NERC's functional model, entities performing these functions have not yet been certified. NERC has historically developed its standards on a control area basis. Because all North American bulk electric systems are monitored by NERC certified control areas and reliability coordinators, the NERC Compliance and Enforcement Program (CEP) will evaluate **only** control areas and reliability coordinators for compliance with this standard. 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 2005, as an update to the self-certification completed in the first quarter of 2004.

Implementation Schedule

2004 — (Assumes Ballot Pool approves extension of Urgent Action Cyber Security Standard)

By August 13, 2004, the NERC Board of Trustees will extend the urgent action cyber security standard through August 13, 2005. The standard remains mandatory for control areas and reliability coordinators for one additional year. Control areas and reliability coordinators ensure that they continue to meet the standard.

NERC and its Regions will develop self-certification renewal forms as part of their compliance and enforcement programs. The Regions will distribute these forms to the control areas 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 control areas and reliability coordinators will be at the entity's discretion.

2005

All control areas and reliability coordinators will complete and submit the appropriate Regional self-certification renewal form(s), indicating their compliance or degree of non-compliance with the requirements of the cyber security standard **during the first quarter of 2005**. 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 NERC Regions and reported to NERC. This data will illustrate whether the industry is substantially compliant with the standard in the beginning of 2005.

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.

Termination

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