NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Compliance Application Notice — DRAFT
Compliance Application: CIP-004-2 R4.2 & CIP-004-3 R4.2

Posted July 30, 2010

Effective Date Month xx, 2010 | *Effective until retired or until a subsequent version of this standard is FERC-approved and enforceable.*

Primary Interest Groups
NERC
Regional Entities
Registered Entities

Issue: Scope of Compliance Application
Registered Entities requested clarification regarding what constitutes revocation of physical and electronic access rights to Critical Cyber Assets (CCAs) as required by CIP-004-2 R4.2 & CIP-004-3 R4.2. Those standards require that a Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

Reliability Objective
Timely revocation of all access rights to CCAs after personnel status changes is necessary to ensure Bulk Electric System reliability.

Clarification:
Registered entities must comply with the requirements that specific physical and electronic access rights to CCAs will be revoked within 24 hours for personnel terminated for cause, and within seven calendar days for personnel who no longer require access to CCAs.

Revocation of access includes all physical and/or electronic access rights that personnel may have to the CCA, regardless of whether the CCA is in a primary, back-up or other environment. This includes, but is not limited to, retrieving and/or disabling or modifying keys, tokens, access cards, badges, smart phones, parking permits, data devices, portable electronic devices, key pads, key passes, passwords, other remote connections and electronic permissions, among other things. Revocation of access rights to CCAs does not include deleting a history of user information or IDs with system or event logs.

With respect to personnel whose access is revoked because they no longer routinely require electronic or physical access to CCAs, such personnel would be treated in accordance with the standard as personnel with unauthorized access, *i.e.*, they must be escorted by authorized personnel when accessing CCAs in accordance with the CIP-006 Reliability Standards, after CCA access is revoked.

While not required by CIP-004-2 R4.2 and CIP-004-3 R4.2, if a registered entity has advance knowledge that a termination for cause will be made, the registered entity may want to consider revocation of physical and electronic access rights concurrent with termination.

Reliability Standards CIP-004-2 and CIP-004-3 do not address the revocation of access to secondary systems and tools that are not CCAs. Revocation of access to secondary access systems and tools that are not within the scope of CIP-004-2 and CIP-004-3 must be included in the registered entity's revocation of access plan.

For more information please contact:

Scott Mix
CIP Technical Manager
scott.mix@nerc.net
609-203-6834

Michael Moon
Director of Compliance Operations
michael.moon@nerc.net
609-524-7028

Suzanna Strangmeier
Senior Standards Interfaces Specialist
suzanna.strangmeier@nerc.net
609-651-7950

This document is designed to convey compliance guidance from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing NERC Reliability Standard. Compliance will continue to be assessed based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this compliance application notice is not a substitute for compliance with requirements in NERC's Reliability Standards. Compliance Application Notices are effective 90 days after their issuance, unless otherwise noted in the Effective Date section. Compliance Application Notices will be reviewed annually and will be modified or retired when the associated NERC Reliability Standard is approved by FERC or other applicable regulatory authorities, revised, or retired, as applicable.