

## Compliance Application Notice – 0007

CIP-004 R4.2 Revocation of Access to Critical Cyber Assets (CCAs)

Posted: December 2, 2010

Revised: December 9, 2011

### Primary Interest Groups

Compliance Enforcement Authority (CEA)<sup>1</sup>

NERC

Regional Entity

Reliability Coordinator (RC)

Balancing Authority (BA)

Interchange Authority (IA)

Transmission Service Provider (TSP)

Transmission Owner (TO)

Transmission Operator (TOP)

Generator Owner (GO)

Generator Operator (GOP)

Load Serving Entity (LSE)

### Issue: What evidence does a CEA seek to determine whether entities revoked access to Critical Cyber Assets (CCAs) as required in CIP-004 R4.2?

For the purpose of aiding a CEA, this CAN provides instruction for assessing whether registered entities revoked access to CCAs as required in CIP-004 R4.2. This CAN also outlines acceptable scenarios for using a technical feasibility exception (TFE).

### Background

Registered entities must comply with CIP-004 R4.2 by revoking access to CCAs within 24 hours for personnel terminated for cause, and within seven calendar days for personnel who no longer require access to CCAs.

Clarification on access: Access to CCAs can be physical, electronic or a combination of both. Access controls for both physical access and electronic access can be used to complement each other to provide increased “defense in depth” (*i.e.*, providing more than one level of control or protection).

Clarification on electronic access: Electronic access allows a user to view, add, update or delete data or information pertaining to Critical Assets or CCAs. In addition, electronic access allows the user to view

<sup>1</sup> Compliance Enforcement Authorities include ERO auditors, investigators, enforcement personnel or any person authorized to assess issues of concern, potential non-compliance, and possible, alleged or confirmed violations of NERC Reliability Standard and requirements.

or manipulate software, system configuration information or database (setting) attributes of a CCA. CEAs are to assess whether electronic access has more than one level or characteristic, such as local, remote, primary or secondary:

- Local electronic access from a directly connected terminal or a computer within the same Electronic Security Perimeter (ESP).
- Remote electronic access in the form of access that is initiated from outside the ESP.
  - Primary electronic access is direct access to the CCA itself.
  - Secondary electronic access involves using additional authentication methods to either gain access to an intermediate system for the purpose of accessing the CCA, or to be authenticated to cross the ESP boundary.

Electronic access control to a CCA could include, but is not limited to, a password, smart-cards or tokens.

Clarification on physical access: Physical access allows a user to access hardware directly and may allow the direct connection of a terminal or a computer that can be used to allow local or primary electronic access. Physical access control to a CCA could include, but is not limited to, devices such as a badge, a key pad, or a key to a door. Some of these examples could also have the ability to include electronic access control elements as well.

Clarification on revocation: Revocation of access to CCAs should result in the inability of an individual to access the CCA. It may include, but is not limited to, removing or disabling user IDs, modifying other systems that prevent the individual from accessing the CCA, or employing a combination of actions. Revocation of access to the CCA also may include revocation of remote access to the CCA coupled with the revocation of physical access to the CCA. Specific actions an entity can take to revoke access will vary, based on the entity and circumstances involved, such as whether the revocation is for personnel terminated for cause or for personnel who no longer require access.

### Compliance Application

CIP-004 provides, in pertinent part:

***R4.** Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.*

...

***R4.2.** The 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.*

CEAs are to look for access to CCAs that is physical, electronic or a combination of both. Access controls for both physical access and electronic access can be used to complement each other to provide increased “defense in depth” (*i.e.*, providing more than one level of control or protection).

An entity may have multiple levels of access control to be revoked to provide “defense in depth.” A CEA is to verify that an individual whose access has been revoked must not be able to access the CCA. This does not mean that all revocations comprising the “defense in depth” strategy must be complete within the specified time frames, but sufficient revocations to deny that entity access to the CCA must be complete within the specified time frames in the standard.

A CEA is to verify either paper or electronic records to indicate revocation of access to CCAs. Such records may include change management documentation, system log files, personnel records, access control lists, asset management records, and other similar documentation. Each of these items must be dated and time-stamped such that CEAs can verify that the minimum timeframes specified in the standard have been met. If a CEA identifies a discrepancy where an individual’s access appears not to have been revoked, the CEA should attempt to verify whether the records are faulty or if the access has actually not been revoked.

A CEA is to use discretion with regard to the type of evidence verified for revocation of access. Actions an entity can take to revoke access will vary, based on the entity and circumstances involved (such as whether the revocation is for personnel terminated for cause or for personnel who no longer require access to CCAs, or based on an entity’s structures, systems, and resulting processes). For example, a dated and time-stamped sign-in sheet documenting the return of a secure access token should be considered valid, as should an electronic log file from a centrally managed system for managing network accounts.

Per the 24-hour requirement of CIP-004 R4.2, CEAs are to look for evidence that registered entities revoked access of individuals terminated for cause within the prescribed 24-hour period. Whether this revocation of access will be physical, electronic, or both will depend on the CCA and will vary, based on the entity’s structures and systems.

While denial of physical access may prevent electronic access to a CCA, a CEA must also verify that other means of accessing a CCA electronically (*i.e.*, local and remote or primary and secondary) are also revoked. If an entity has an approved TFE in place that prohibits activity that may normally be required to revoke access, such as changing a generic password, the TFE must include mitigation controls that address revocation of access. CEAs must verify during audits that mitigation controls are in place.

### **Examples**

Examples of revoking electronic access can include, but are not limited to, disabling electronic permissions or other actions as appropriate. Revoking physical access can include, but is not limited to,

retrieving a hard key, modifying or changing physical access components such as locks or badge systems, and inhibiting the terminated user's ability to use visitor or lost-badge procedures to procure a replacement badge. Where remote access is provided using shared or generic User IDs, appropriate procedural controls should be applied to revoke access for personnel who have been terminated or who no longer require access. Disabling any remote connectivity capability and revoking information and authentication mechanisms that allow for remote access also can be considered. Revoking electronic access includes removing the ability to remotely access the CCA (*i.e.*, removing the ability to access across the Electronic Security Perimeter) along with the revocation of physical access to the CCA.

For Microsoft®-based operating platforms that participate in "domains," revocation actions may be accomplished by revoking domain access. For non-Microsoft based operating platforms and non-centralized stand-alone Microsoft-based platforms, actions to revoke access may vary from entity to entity based on system differences, but must meet the objective to revoke access in compliance with the requirement. A CEA is to verify that access was revoked by a combination of revocation of physical access, electronic access and remote access.

Revocation may not necessarily require deletion of all access elements, such as User IDs. In some systems, such as Unix, User IDs may be used for remote or electronic access as well as to maintain additional information distinctly separate, such as object ownership and resource accounting information. In these cases, entities should exercise caution and not remove User IDs based on revocation of individual access. Rather, the User ID should be disabled without deleting it, thereby revoking access. Additionally, CEAs are to identify whether system and event logs associated with the User ID being disabled were preserved consistent with the requirements of CIP-005 R5.3 and CIP-007 R6.

### **Effective Period for CAN**

This revised CAN supersedes the original CAN, as well as all prior communications. CEAs are to use this CAN to assess compliance from December 2, 2010, regardless of the start date of the violation. It will remain in effect until such time that a future version of the standard or interpretation addresses the specific issue contained in this CAN and is enforceable.

For any enforcement action in process and for audits that have been initiated,<sup>2</sup> a CEA is to apply the appropriate discretion, including consideration of the specific facts and circumstances of the non-compliance, in determining whether to assess compliance pursuant to this CAN.

### **Evidence of Compliance**

A CEA is to assess the following to obtain reasonable assurance of the entity's compliance as described above:

---

<sup>2</sup> "Initiated" means that a registered entity has received notification of the upcoming audit.

For employees terminated for cause, a CEA is to look for, at a minimum:

- Human Resources’ or other corporate documentation of the date of termination
- Evidence that access was revoked within 24 hours of the date of termination

For employees who no longer require access to CCAs, a CEA is to look for, at a minimum:

- Human Resources’ or other corporate documentation of the date on which the employee no longer required access
- Evidence that revocation occurred within seven days of the date on which the employee no longer required access

For more information please contact:

Michael Moon  
 Director of Compliance Operations  
[michael.moon@nerc.net](mailto:michael.moon@nerc.net)  
 404-446-2567

Scott Mix  
 CIP Technical Manager  
[scott.mix@nerc.net](mailto:scott.mix@nerc.net)  
 215-853-8204

*This document is designed to convey compliance monitoring instruction to achieve a measure of consistency among auditors and Compliance Enforcement Authorities. 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 currently enforceable NERC Reliability Standards. This document is not intended to define the exclusive method an entity must use to comply with a particular standard or requirement, or foreclose a registered entity’s demonstration by alternative means that it has complied with the language and intent of the standard or requirement, taking into account the facts and circumstances of a particular registered entity. Implementation of information in this document is not a substitute for compliance with requirements in NERC’s Reliability Standards.*

**Revision History**

Posted Date	Action	Revision
October 25, 2010	Posted Final CAN	
December 9, 2011	Posted Revised CAN	Revised target audience to CEAs