

Compliance Application Notice – 0005

CIP-002 R3 Critical Cyber Asset Designation for System Operator Laptops

Posted: October 1, 2010

Revised: March 24, 2011

Revised: July 6, 2011

Revised: December 9, 2011

Primary Interest Groups

Compliance Enforcement Authority (CEA)¹

NERC

Regional Entity

Balancing Authority (BA)

Generator Operator (GOP)

Generator Owner (GO)

Interchange Authority (IA)

Load Serving Entity (LSE)

Reliability Coordinator (RC)

Transmission Service Provider (TSP)

Transmission Operator (TOP)

Transmission Owner (TO)

Issue: Must system operator laptops with the capability and purpose of remotely controlling Critical Assets be considered Critical Cyber Assets (CCAs)?

For the purpose of aiding CEAs, this CAN provides instruction for assessing whether system operator laptops² with the capability and purpose of controlling Critical Assets remotely (either in normal operations or in emergencies) should be designated as CCAs.

Background

This CAN has been revised from the July 06, 2011 version based on direction from the NERC Board of Trustees provided at the August 3, 2011 meeting. The direction stated that CANs are to provide instruction to CEAs. Additionally, the CAN was modified after further analysis of the impact on reliability resulting from registered entities' responses to the wording in the previous CAN. It is impractical for a CAN to attempt to identify applicability given the multitude of situations in which various laptops may

¹ 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.

² System operator laptops include, but are not limited to, any portable device used by a system operator, including notebooks, netbooks, tablets, or PDA devices, whether wired or wireless, with the capability and purpose of controlling Critical Assets remotely, as described above. The scope of CAN-0005 is limited to these categories of laptops.

have the “capability and purpose to control critical assets,” and therefore, it was concluded that the registered entity is in the best position to make the determination of which laptops are used as a CCA.

Compliance Application

CIP-002-3 provides, in pertinent part:

***R3. Critical Cyber Asset Identification** — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:*

***R3.1.** The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,*

***R3.2.** The Cyber Asset uses a routable protocol within a control center; or,*

***R3.3.** The Cyber Asset is dial-up accessible.*

CEAs are to verify that registered entities followed their own internal back-up, emergency and evacuation procedures to properly identify Cyber Assets that are essential to the reliable operation of Critical Assets as Critical Cyber Assets, including normal, backup and emergency operations. This may or may not include identification of system operator laptops or other remote access technology as Critical Cyber Assets.

In the event that a Cyber Asset that is essential to the reliable operation of a Critical Asset, based on a review of the entity’s back-up, emergency and evacuation procedures, is not identified as a Critical Cyber Asset, a CEA is to find a Possible Violation.

A CEA will be required to make this determination based on his professional judgment, as well as the facts and circumstances that exist in the registered entity’s environment. A CEA is also to consider a registered entity’s rationale for identifying Critical Cyber Assets.

Effective Period for CAN

This CAN is effective upon posting as final on the NERC Web site and is to be used by CEAs to assess compliance from the posting date forward, regardless of the start date of any non-compliance or Possible Violation. It supersedes all prior communications and prior versions of CAN-0005 and will

remain in effect until such time that a future version of a FERC or other applicable government authority approved standard or interpretation becomes effective and addresses the specific issue contained in this CAN.

For any enforcement action in process and for audits that have been initiated,³ a CEA will 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

CEAs are to verify the following evidence for reasonable assurance of compliance:

- The registered entity's list of Critical Cyber Assets;
- A registered entity's process for identifying Critical Cyber Assets, which may be a documented procedure, or, if the entity does not have a documented procedure, through interviews with personnel and other supporting evidence.

Also, the CEA is to verify that the registered entity's list of Critical Cyber Assets is complete pursuant to the registered entity's identification process.

For more information please contact:

Michael Moon
Director of Compliance Operations
michael.moon@nerc.net
404-446-2567

Valerie Agnew
Manager of Interface and Outreach
valerie.agnew@nerc.net
404-446-2566

Scott Mix
CIP Technical Manager
scott.mix@nerc.net
215-853-8204

Tom Hofstetter
CIP Compliance Specialist
tom.hofstetter@nerc.net
609-651-2532

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.

³ "Initiated" means that a registered entity has received notification of the upcoming audit.

Revision History

Posted Date	Action	Revision
October 1, 2010	Posted Final CAN	
March 24, 2011	Posted Revised CAN	Superseded October 1, 2010 version
July 6, 2011	Posted Revised CAN	Superseded all prior versions
December 9, 2011	Posted Revised CAN	Revised target audience to CEAs; supersedes all prior versions