

Compliance Application Notice — 0005

CIP-002-3 R3 Critical Cyber Asset Designation for System Operator Laptops

Posted: October 1, 2010

Revised: March 24, 2011

Revised: July 06, 2011

Revised: August XX, 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: Are system operator laptops with capability to remotely control Bulk Power System (BPS) assets 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 BPS assets remotely (either in normal operations or in emergencies) should be designated as CCAs.

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 Bulk Electric System assets remotely, as described above.

Background

The practice of when to designate a laptop as a CCA has differed among registered entities and Regional Entities. Some entities have designated laptops as CCAs if the laptop can remotely access and control CCAs and non-CCAs that reside in an Electronic Security Perimeter (ESP), while others have not.

NERC recognizes the need for flexibility in allowing remote access to ensure electric system reliability, as well as the requisite obligation to designate the laptops as described above as CCAs to ensure BPS reliability.

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 system operator laptops with the capability and purpose of controlling Critical Assets remotely (either in normal operations or in emergencies) are designated as CCAs under CIP-002-3 Requirement R3.

These laptops provide essential functionality for operation of Critical Assets similar to back-up control centers. While these laptops, as described above, significantly enhance electric system reliability by providing redundant and diverse capability and communications paths, their use can impact the reliable operation of a Critical Asset that is essential to reliable operations.

As of January 1, 2011 (90 days after the original posting date of CAN-0005), CEAs are to treat system operator laptops with the capability and purpose of controlling Critical Assets remotely (either in normal operations or in emergencies) as CCAs, and as such, all Critical Infrastructure Protection (CIP) Standards must be adhered to for these devices. This places an appropriate focus on cyber security in accordance with the suite of CIP standards.

Effective Period for CAN

This revised CAN supersedes all prior versions of CAN-0005 on the topic of remote laptops. CEAs are to use this CAN to assess compliance from January 1, 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,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.

Future efforts are underway to refine NERC Reliability Standards for remote access, including the Reliability Standards Project 2008-06 Cyber Security 706 and Project 2010-15: Urgent Action Revisions to CIP-005-3.⁴ This CAN does not address compliance or noncompliance issues with respect to other systems, configurations or devices, and they may similarly be subject to enforcement action in accordance with the CIP Standards.

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
 404-446-2567

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

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

Date	Action
October 1, 2010	Posted Final CAN-0005
March 24, 2011	Posted Revised CAN-0005 that Superseded October 1, 2010 version
July 6, 2011	Posted Revised CAN-0005 that Superseded all previous versions
August XX, 2011	Posted Revised CAN-0005 that Superseded all previous versions

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

⁴ http://www.nerc.com/docs/standards/sar/Project_2010-15_SAR_to_Revise_CIP-005-3_Using_Expedited_Process_20101105.pdf