

Compliance Application Notice — 0005

~~Compliance Application: CIP-002_3-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~~

~~Re-Posted July 06, 2010 and March 24, 2011~~

~~Effective October 1, 2010¹~~

Primary Interest Groups

~~Compliance Enforcement Authority (CEA)²~~

~~NERC~~

~~Regional Entity~~

~~Balancing Authorities Authority (BA)~~

~~Load Serving Entities~~

~~Transmission Service~~

~~Providers~~

~~Generator Operators Operator (GOP)~~

~~NERC~~

~~Transmission Operators~~

~~Generator Owners Owner (GO)~~

~~Regional Entities~~

~~Transmission Owners~~

~~Interchange Authorities Authority (IA)~~

~~Reliability Coordinators~~

~~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)? Compliance Clarity & Consistency**~~

~~For the purpose of aiding CEAs, this CAN provides instruction for assessing Registered entities and Regional Entities requested clarity regarding whether system operator laptops³ with the capability and~~

¹ ~~Effective until retired or until a subsequent version or interpretation of this standard that addresses this issue is FERC approved and enforceable.~~

² ~~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.~~

Formatted: Indent: Left: -0.5", Don't adjust space between Latin and Asian text

purpose of controlling ~~Critical Assets remotely (Bulk Electric System assets remotely (whether in normal operations or in emergencies) should be designated as Critical Cyber Assets (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 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 System operator laptops with the capability and purpose of controlling Critical Assets as Critical Cyber~~

³ 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.

Formatted: Indent: First line: 0"

~~Assets, including normal, back-up and emergency operations. This may or may not include identification of system operator remotely (whether in normal operations or in emergencies) should be designated as CCAs under CIP-002-3 Requirement R3. Registered entities should consider this guidance when developing and using its risk-based assessment methodology to designate Critical Assets and associated CCAs. These laptops or other remote access technology as Critical Cyber Assets. 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. 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,⁴ 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.~~

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 CCAs and non-~~

Formatted: Indent: Left: -0.5"

Formatted: Indent: Left: -0.5", Don't adjust space between Latin and Asian text

Formatted: Indent: Left: -0.5"

Formatted: Indent: Left: -0.5", Don't adjust space between Latin and Asian text

Formatted: Indent: Left: -0.25", Don't adjust space between Latin and Asian text

Formatted: Indent: Left: -0.5", Don't adjust space between Latin and Asian text

⁴ "Initiated" means that a registered entity has received notification of the upcoming audit.

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 electric system reliability. As of ninety days after the posting date of this Compliance Application Notice, October 1, 2010, NERC compliance monitoring and enforcement activities will treat system operator laptops with the capability and purpose of controlling critical assets remotely (whether in normal operations or in emergencies) as CCAs, and as such, all Critical Infrastructure Protection Standards must be adhered to for these devices. This places an appropriate focus on cyber security in accordance with the suite of Critical Infrastructure Protection standards. 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-005-3.⁵ 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 Critical Infrastructure Protection Standards.

For more information please contact:

Scott Mix CIP Technical Manager scott.mix@nerc.net 609-203-6834	Tom Hofstetter CIP Compliance Specialist tom.hofstetter@nerc.net 609-651-2532
--	---

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

Valerie Agnew
Manager of Compliance Standards-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.

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 Standards. Compliance will continue to be determined 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.

Formatted: Indent: Left: -0.5"

⁵ http://www.nerc.com/docs/standards/sar/Project_2010-15_SAR_to_Revise_CIP-005-3_Using_Expedited_Process_20101105.pdf

Revision History

<u>Posted Date</u>	<u>Action</u>	<u>Revision</u>
<u>October 1, 2010</u>	<u>Posted Final CAN</u>	
<u>March 24, 2011</u>	<u>Posted Revised CAN</u>	<u>Superseded October 1, 2010 version</u>
<u>July 6, 2011</u>	<u>Posted Revised CAN</u>	<u>Superseded all prior versions</u>
<u>December 9, 1011</u>	<u>Posted Revised CAN</u>	<u>Revised target audience to CEAs; supersedes all prior versions</u>

Formatted: Indent: Left: -0.5"

Formatted Table