NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Industry Advisory

Remote Access Guidance

Initial Distribution: August 24, 2011

Vulnerabilities for remote access methods and technologies previously thought secure and in use by a number of large electric sector entities, may require changes to industry security control practices.

Why am I receiving this? >>
About NERC Alerts >>

Status:	**No Reporting is Required – For Information Only**
	PUBLIC: No Restrictions **More on handling >>**
Instructions:	NERC Advisories are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure, for such use as your organization deems appropriate. **No particular response is necessary.** This NERC Advisory is not the same as a reliability standard, and your organization will not be subject to penalties for a failure to implement this Advisory. Additionally, issuance of this Advisory does not lower or otherwise alter the requirements of any approved Reliability Standard, or excuse the prior failure to follow the practices discussed in the Advisory if such failure constitutes a violation of a Reliability Standard.
Distribution:	**Primary Distribution:** Primary Compliance Contacts**,** All Functional Entities **Who else will get this alert? >>** **What are my responsibilities? >>**
Primary Interest Groups:	Information technology, cyber security, network administration, control system support, substation technicians, plant operations.
Advisory:	NERC Standard Development Project 2010-15 developed a Secure Interactive Remote Access guidance document, a modified version of which is associated with this Industry Advisory. Registered Entities are requested to implement the following recommendations for secure remote interactive access as further explained in the guidance document associated with this Advisory. Entities should employ judgment to develop an effective solution which implements as many of the recommendations as practical. The recommended methods for secure interactive remote access include: 1. Using encrypted and securely authenticated access controls when

interactively remotely accessing control and monitoring systems. (See also recommendation #4.)

2. Utilization of multi-factor (two or more factors) when authenticating users of interactive remote access. (See also recommendation #4.)
3. Ensuring that accounts used for interactive remote access are either a) different accounts specifically provisioned for interactive remote access, or b) existing accounts are specifically authorized to allow interactive remote access. Accounts should be provisioned on an individual basis.
4. Implementation of an intermediate device (sometimes called a proxy server or "jump host") as a VPN/encryption termination device, and multi-factor authentication device.
5. Prohibition of "VPN Split Tunneling" and network dual-hosting on systems used to interactively remotely access control systems.
6. Ensuring that remote computers used to initiate interactive remote access are running up-to-date patches and anti-malware software.
7. Implementing an inactivity timeout to automatically disconnect the remote interactive access after a pre-defined (and entity-specified) period of inactivity.
8. As an alternative to providing interactive remote access from general-use remote computers, utilizing a securely configured read-only boot device (such as a bootable CD or bootable read-only USB disk) to initiate remote access from non-company controlled remote computers.
9. Implementing logging and monitoring of all user activity including file transfers and program activation at the access point, as part of the proxy server, or with a specialized device for accountability.
10. Implementing an account lock-out feature such that an account is locked out for a period of time following a pre-determined number of repetitive, unsuccessful login attempts.

The associated guidance document provides additional details, suggestions and case studies for interactive remote access methods when remotely accessing control systems. The practices listed in the guidance document are neither all inclusive nor exhaustive; various examples may apply to one type of entity and not to another.

Failure to properly secure and control remote access to Cyber Assets used to control or monitor Bulk Electric System facilities or elements could lead to misuse of facility and element controls and loss of monitoring functions, leading to unintended outages or equipment damage.

The ES-ISAC estimates that the risk to bulk power system reliability from this vulnerability is MEDIUM, due to the potential for misuse of remotely accessed systems.

Background:	Recent discovery and announcement of vulnerabilities for remote access methods and technologies, that were previously thought secure and in use by a number of large electric sector entities, necessitate important changes to industry security control practices. Currently, no NERC Standards

NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

requirements or guidance documents are available to either require or recommend how secure remote access to Cyber Assets (whether they are Critical Cyber Assets, non-Critical Cyber Assets, or other assets used for access control and monitoring) can or should be accomplished. This Industry Advisory provides a set of recommendations for configuring secure remote access to those Cyber Assets. An associated supplementary guidance document provides additional details and best practice use-cases of in-place implementations to show how secure remote access may be implemented by a Responsible Entity.

See attachment "Guidance for Secure Interactive Remote Access."

Please note that all inquiries regarding this advisory can be addressed to the following NERC Staff.

Contact:

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

To report any incidents related to this alert, contact:
ES-ISAC 24-hour hotline
609.452.1422
esisac@nerc.com

A-2011-08-24-01

North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560 www.nerc.com