

# Security Guidelines for the Electricity Sector: Cyber — Access Controls

<b>NERC</b>	<b>Guideline</b>
<b>Guideline Title: Cyber — Access Control</b>	<b>Version: 1.0</b>
Revision Date:	Effective Date: June 14, 2002

## **Purpose:**

The purpose of this guideline is to provide for a minimum baseline for secure cyber access control across the electric sector. This guideline identifies some of the key elements associated with managing access to information systems and services vital to maintaining the reliability of the electric infrastructure. Such access includes logical access to computers and networks, as well as access to the physical environments where computer and network equipment is located — i.e. computer rooms, etc.

## **Applicability:**

This guideline is applicable to anyone who owns and/or manages information systems and/or services that support the electric infrastructure.

A computer system environment is as critical as its most critical component and as vulnerable as its most vulnerable component. Therefore this guideline would be applicable across the enterprise.

## **Guideline Statement:**

Effective access controls are critical to protecting electronic information systems and services that support and maintain the electric infrastructure. Anyone who owns and/or manages information systems and/or services that support the Electric Infrastructure should have documented policies and procedures in place to manage authorization, authentication, and monitoring of logical and physical access to such information systems and services. Such documentation should clearly define roles and responsibilities, procedures for establishing authorization, and the methods you select for authentication and monitoring.

## **Guideline Detail:**

### ***Authorization***

There should be a process that requires signatory approval for any individual to have logical or physical access to information systems and services. This process should address:

# Security Guidelines for the Electricity Sector: Cyber — Access Controls

Identification of individual being granted access (USER)

- USER sign-off, agreeing to abide by all applicable information and access policies and procedures
- USER role description, business justification for access being granted
- Specific systems, servers, and/or databases to be accessed
- Any constraints, limitations on access granted
- Identification of person responsible/accountable for the system, server, database, and/or physical/restricted area to be accessed (OWNER)
- Signatory approval of OWNER
- A date for access to be terminated or a signed renewal of authorization. (Recommended to be not more that one year.)

## ***Authentication***

Any access that allows any command or control of a system, application, or database, or allows any add, modify, delete, or transmittal of any data, should utilize some method for authenticating the USER. Methods of authentication are typically based on something you know, something you have, or something you are. The strength of the method implemented may vary depending on the sensitivity and degree of risk associated with the access granted. Implementing two or more methods simultaneously can increase the strength of authentication, such as utilizing something you know with something you have. Today's field of authentication solutions ranges greatly, to include:

- Basic lock and key (Primarily Physical)
- Simple passwords (Primarily Logical)
- Electronic Badges/Smart Cards (Logical and Physical)
- Cryptography (Handheld, Digital Signatures, etc.) (Logical and Physical)
- Bio-metrics (Logical and Physical)

# Security Guidelines for the Electricity Sector: Cyber — Access Controls

## ***Monitoring***

The most basic level of monitoring dictates an effective audit trail. A good audit trail will support enforcement of USER accountability and aid an OWNER in validating USER trust.

For logical access, system and application logs are the primary means for establishing a good audit trail. These logs should identify:

- The date and time an access was authenticated
- The USER that was authenticated
- USER initiated events, such as commands and programs initiated
- The date and time of the event
- The date and time the USER access was terminated

For physical access to computer rooms, etc., a formal assessment may be appropriate to determine if the degree of risk warrants activity logging. If logging is determined to be a requirement, such logs should be able to identify the USER and date/time of both entry and egress. There are a variety of electronic lock solutions available that will support such logging. If activity logging is also desired, video monitoring appears to be the most viable solution at this time.

## **Related Documents:**

- *Information Security Primer*, Electric Power Research Institute, April 2001  
<http://www.nerc.com/~filez/cipfiles.html>
- *An Introduction to Computer Security: The NIST Handbook*, National Institute of Standards and Technology, October 1995  
<http://csrc.nist.gov/publications/nistpubs/800-12>
- NIST Special Publications, NIST documents of general interest to the computer security community,  
<http://csrc.nist.gov/publications/nistpubs/index.html>
- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
  - Vulnerability and Threat Assessment
  - Threat Response

# Security Guidelines for the Electricity Sector: Cyber — Access Controls

- Emergency Plans
- Continuity of Business Processes
- Communications
- Physical Security
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

— *An Approach to Action for the Electricity Sector, Version 1*, NERC, June 2001, <http://www.nerc.com>

— *Threat Alert Levels and Physical Response Guidelines*, NERC, November 2001, <http://www.nerc.com>

— *Threat Alert Levels and Cyber Response Guidelines*, NERC, March 2002, <http://www.nerc.com>

## Revision History:

Date	Version Number	Reason/Comments