

# Security Guidelines for the Electricity Sector: Cyber — IT Firewalls

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

## **Purpose:**

An understanding of firewalls and firewall technology is critical for any Information Technology and Services organization to successfully implement and maintain an acceptable level of security. This document identifies some resources that are available for an IT organization to develop an understanding of firewalls and firewall policies that will help mitigate cyber risks to its computing infrastructure.

## **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:**

To implement and maintain a successful firewall program today requires a proactive, ongoing effort. As technology changes, so do the tools used for network attacks. It is imperative that IT organizations remain current with changes in technology to understand new attack methods and tools, and to identify new methods and tools to counter-act them.

The National Institute of Standards and Technology has published a guide titled, "Guidelines on Firewalls and Firewall Policy." It is recommended that IT organizations that support the electric infrastructure review this document, and other available documentation in developing their own firewalls program.

It should be noted that simply installing one or more firewalls is not sufficient. Staff needs to be dedicated to managing the firewall rules and evaluating the firewall logs for suspicious activity. Also, the NIST guidelines' recommendations for a layered defense (Internet firewall, DMZ/Internal firewall, network segmentation internal firewalls, and using multiple vendors) should be seriously considered.

# Security Guidelines for the Electricity Sector: Cyber — IT Firewalls

## Related Documents:

- *Guidelines on Firewalls and Firewall Policy*, National Institute of Standards and Technology, Special Publication 800-41, January 2002  
<http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf>
- NIST Special Publications, NIST documents of general interest to the computer security community,  
<http://csrc.nist.gov/publications/nistpubs/index.html>
- *Information Security Primer*, Electric Power Research Institute, April 2001  
<http://www.nerc.com/~filez/cipfiles.html>
- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
  - Vulnerability and Threat Assessment
  - Threat Response
  - 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