

Security Guidelines for the Electricity Sector: Cyber — Intrusion Detection

NERC	Guideline
Guideline Title: Cyber — Intrusion Detection	Version: 1.0
Revision Date:	Effective Date: June 14, 2002

Purpose:

An understanding of cyber intrusion detection technology and methods 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 intrusion detection systems 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 cyber intrusion detection 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 those attacks when they occur.

The National Institute of Standards and Technology has published a guide titled, "Intrusion Detection Systems." It is recommended that IT organizations that support the electric infrastructure review this document and other available documentation in developing their own intrusion detection program.

It should be noted that simply installing an intrusion detection system is not sufficient. Staff needs to be dedicated to manage IDS rule sets and monitor/evaluate the logs and alarms for suspicious activity. This is a non-trivial activity that cannot be done on an occasional basis. Early detection is essential and staffing at the 24x7 level should be considered. Automated monitoring

Security Guidelines for the Electricity Sector: Cyber — Intrusion Detection

alarms that initiate alerts tied to pager, email, and/or voice messaging systems also should be considered.

Related Documents:

- *Intrusion Detection Systems*, National Institute of Standards and Technology, Special Publication 800-41, November 2001
<http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>
- *Information Security Primer*, Electric Power Research Institute, April 2001
<http://www.nerc.com/~filez/cipfiles.html>
- 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
 - 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

Version 1.0
June 14, 2002

Security Guideline: Cyber —
Intrusion Detection
Page 2 of 2