

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

NERC	Guideline
Guideline Title: Vulnerability and Risk Assessment	Version: 1.0
Revision Date:	Effective Date: June 14, 2002

Purpose:

A vulnerability and risk assessment helps identify critical facilities as well as their vulnerabilities. Such an assessment also helps identify countermeasures to mitigate threats.

Each company must assess the need to conduct a Vulnerability and Risk Assessment within the context of its operating environment.

Applicability:

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual company.

Each company is free to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility through redundancies may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

Guideline Statement:

This guideline recommends “best practices” for the electricity sector in the area of “Vulnerability and Risk Assessment” for facilities and functions identified as critical.

Table of Contents:

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

Guideline Detail:

Vulnerability analyses and risk assessments provide a method of prioritizing the criticality of assets (or the impact of the loss of the asset), threats, and countermeasure strategies. A structured risk assessment process allows for the documentation by subject matter experts based on their judgments and assumptions. The final product is a broad set of priorities, both physical and cyber, that contribute to the protection of the critical systems or functions.

In many cases a checklist survey is used in conducting a risk and vulnerability assessment. The checklist includes an overview of a fairly standard approach to concepts of risk assessment, and includes questions and considerations for use during each step of the process. Cyber as well as physical security should be assessed during this survey.

An Outline Of Analytical Risk Management Steps

The following is an outline of a standard risk management process primarily used to assess vulnerabilities and to assist in the prioritization of developing countermeasures to mitigate the vulnerabilities identified. There are many other models, and companies should choose the model that best fits their operational environment. There are four steps to this process.

1. Identification of assets and loss impacts.
 - a. Determine the critical assets that require protection.
 - b. Identify possible undesirable events and their impacts.
 - c. Prioritize the assets based on consequence of loss.
2. Identification and analysis of vulnerabilities.
 - a. Identify potential vulnerabilities related to specific assets or undesirable events.
 - b. Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities.
 - c. Estimate the degree of vulnerability relative to each asset.

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

3. Assessment of risk and the determination of priorities for the protection of critical assets.
 - a. Estimate the degree of impact relative to each critical asset.
 - b. Estimate the likelihood of an attack by a potential adversary.
 - c. Estimate the likelihood that a specific vulnerability will be exploited. This can be based on factors such as prior history or attacks on similar assets, intelligence, and warning from law enforcement agencies, consultant advice, the company's own judgment, and additional factors.
 - d. Prioritize risks based on an integrated assessment.
4. Identification of countermeasures, their costs and trade-offs.
 - a. Identify potential countermeasures to reduce the vulnerabilities.
 - b. Estimate the cost of the countermeasures.
 - c. Conduct a cost-benefit and trade-off analysis.
 - d. Prioritize options and recommendations for senior management.

Using a vulnerability and risk assessment survey tool may be useful for the following:

- prioritizing critical assets and identification of vulnerabilities
- prioritizing risks and their priorities, and
- prioritizing countermeasures.

Following are general considerations that may be taken into account when conducting a risk and vulnerability assessment.

- Develop a process to identify critical electric infrastructure systems and facilities both from a physical and cyber security perspective.
- Identify protection and assurance responsibilities for cyber and physical security and whether there are gaps or overlaps among these responsibilities

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

- Coordinate security response requirements with law enforcement officials at the appropriate federal, regional, and local levels to assure good communication and coordination in protecting the critical infrastructure facilities.
- Develop an emergency management response process to reduce or mitigate impacts of a loss of electric supply or deliverability (see guideline on emergency planning).
- Prepare a formal mutual assistance agreement at the appropriate local, state, or regional level to support response, repair, and restoration activities for the disrupted critical infrastructure facility.

Consider interdependencies among infrastructures when evaluating the consequences of a cyber or physical security incident. An incident in one infrastructure can cascade to failures in other infrastructures.

Also consider coordinating contingency response plans with other infrastructure entities and sectors to assure coordination during emergencies.

Exceptions:

Certified Products/Tools:

Related Documents:

- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
 - Threat Response
 - Emergency Plans
 - Continuity of Business Processes
 - Communications

Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment

- 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

ARCHIVED