

# Security Guidelines for the Electricity Sector: Emergency Plans

<b>NERC</b>	<b>Guideline</b>
<b>Guideline Title: Emergency Plans</b>	<b>Version: 1.0</b>
Revision Date:	Effective Date: June 14, 2002

## **Purpose:**

Emergency plans ensure that a company is prepared to respond to a spectrum of threats ranging from simple trespassing, to vandalism, to civil disruptions, to dedicated acts of terror and sabotage by perpetrators inside and outside the company whose actions may be cyber or physical in nature.

Emergency plans typically address training of key participants to ensure they have the skills and knowledge to effectively carry out those plans. The extent to which emergency planning occurs will vary for each company depending on the results of its Vulnerability and Risk Assessment and its perceived spectrum of threats.

## **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 “Emergency Plans” for facilities or functions considered critical.

# Security Guidelines for the Electricity Sector: Emergency Plans

## Table of Contents:

### Guideline Detail:

Many companies in the electricity sector have emergency plans in place that are used regularly to respond to storms, hurricanes, floods, tornadoes, earthquakes, and other emergencies. These same plans can be used to respond to incidents caused by an expanding “spectrum of threats,” including terrorism or other manmade disasters.

Effective emergency plans typically include the following:

- “Formal mutual assistance agreements” which include notification of law enforcement and state emergency preparedness officials should be in place.
- Contingency plans that are appropriate and flexible for addressing incidents at system control centers, critical substations, and generation stations should be in place.
- A formal and defined emergency management process to mitigate physical and cyber security incidents and restore service quickly. Plans should include the identification, procurement, and proper security for critical spare parts.
- A notification process for employees, contractors, and vendors. Well informed personnel are a company’s first line of defense for observing and reporting suspicious activities in and around their facilities or their information technology (IT) systems.
- Emergency preparedness plans that address cyber and physical security counter measures when threat information is received from the NIPC, ES-ISAC, or other agency.
- A training and orientation program for key responders should be developed and periodically reviewed. Periodic exercises may include tabletops with stretching scenarios and include first responders from law enforcement, fire, and state authorities when appropriate. (Many companies involve local agencies in some of their emergency exercises and training but reserve the right to conduct exercises on their own to ensure more candor in the process.) At the conclusion of all exercises, a comprehensive “lessons-learned” critique should be conducted and results incorporated into the emergency plans. Additionally, the exercise “lessons-learned” should be used as a basis for future training and orientation sessions.

## **Security Guidelines for the Electricity Sector: Emergency Plans**

The following elements should be considered for inclusion in an overall company emergency plan:

- A broad description of the Emergency Management Organization (EMO).
- A general description of emergency response priorities (protecting life, property, restoring services, etc.).
- Identification of a person or group responsible for the development, maintenance, and testing of the overall emergency plan.
- A requirement that the plan be updated on a periodic basis.
- A requirement that the plan be tested at least annually.
- A requirement for a critique or debriefing session be conducted after exercises and significant emergency events and that plans be modified based on the results of those critiques and documented “lessons learned.”

Other company emergency plans should be consistent with, and coordinated under, the overall company emergency plan.

Although terrorist incidents are covered under the general umbrella of the emergency plan, there may be value in adding a security element to existing emergency plans that reflect contingency plans that would be put in place consistent with the NERC Physical and Cyber Threat Alert Levels.

Each company should consider having an Emergency Operations Center known to emergency management team members. That center does not necessarily have to be a dedicated center but could be an existing office or conference space that can be readily converted into an emergency center. Consideration should also be given to an alternate emergency center for use in the event that the first center is unavailable. Both a primary and an alternate Emergency Operation Center should have:

- standby power as well as sufficient information and communication infrastructure to support emergency operations;
- sufficient resources to manage an emergency including clerical support, operating diagrams, manuals, and other reference materials; and
- a person designated as responsible for the update and maintenance of the emergency center and its alternate.

# Security Guidelines for the Electricity Sector: Emergency Plans

Each company should consider designating an Emergency Management Team (EMT). That team should have representation from the following:

- Operations (Generation, Transmission, Distribution).
- External Communications (External Relations, Customer Services, Call Center Operations, Human Resources, and others).
- Logistics (Facilities, Materials, IT Support, etc.).
- Finance (Controller, Banking, etc.)
- Security
- Information Technology

An EMT should have a clearly designated emergency team leader (typically a member of senior management) as well as alternates in the event the team leader is not be available or extended emergencies require multiple shifts.

Companies should make sure that countermeasures, both physical and cyber, are identified in their plans and reviewed at the time a threat warning is received. Countermeasures speed recovery in a comprehensive, systematic, and planned manner.

Emergency plans should contain “a lessons-learned provision” to be used whenever the Emergency Management Organization is activated whether it be caused by a security threat or a natural disaster. Consideration should be given to applying lessons learned from natural disasters to security incidents contingencies.

The response plans should be flexible enough to adapt to various levels of threat, i.e., intelligence information received from the NIPC which indicates a local or regional threat versus a general threat statement issued encouraging all utilities to take proactive deterrent measures. The more localized and specific the threat, the more security countermeasures, both cyber and physical, should be considered by the Emergency Management Organization (EMO).

## **Exceptions:**

# Security Guidelines for the Electricity Sector: Emergency Plans

## Certified Products/Tools:

## Related Documents:

- Security Guidelines for the Electricity Sector: Guideline Overview
- Security Guidelines for the Electricity Sector:
  - Vulnerability and Threat Assessment
  - Threat Response
  - 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