

# Security Guidelines for the Electricity Sector: Communications

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

## **Purpose:**

Each company should consider establishing an effective liaison relationship with its local offices of federal, regional, and local law enforcement agencies, especially in the areas where critical facilities are located. Where feasible, provide familiarization tours for law enforcement agencies having jurisdiction in areas where critical facilities are located, and conduct pre-planning and coordination for potential response scenarios. This liaison should be periodically updated and verified to ensure that contact information and facility familiarization is current.

Each company should be able to ensure that company personnel can respond to alarms, outages, or other issues at critical operating facilities. This might include the availability of robust communications systems such as radio, cellular phone, or other communications devices. Additionally, a system of communicating threat warnings to appropriate organizations within the company should be developed, along with appropriate actions to implement based upon the declared threat level.

Each company should report security related incidents promptly within the company as well as to local enforcement agencies. Those incidents falling within the NERC threat-reporting guidelines should also be reported promptly to the National Infrastructure Protection Center (NIPC) and the ES-ISAC.

## **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

# Security Guidelines for the Electricity Sector: Communications

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 infrastructure in the area of “Communications” for facilities or functions considered critical.

## **Table of Contents:**

## **Guideline Detail:**

Companies should consider implementing the following items to assure timely and proper response by law enforcement organizations to a security incident.

1. Establishing contact with (for example) the Key Asset Program Coordinator or InfraGard Coordinator of the FBI Division Headquarters for your service territory (Note: in large geographic areas or for companies operating in multiple states, several FBI Divisions may need to be contacted).
2. Participation by US entities in the FBI InfraGard Program.
3. Developing liaison with the State Police, National Guard, Office of Emergency Preparedness, and State Homeland Security Office or equivalent.
4. Developing liaison with officials having regional mutual aid jurisdiction (generally the Sheriff's Dept.) and any regional law enforcement groups that represent multi-agency coordination as well as with the local law enforcement agencies having direct jurisdiction near critical facilities.
5. Providing pre-planning familiarization tours of critical sites to law enforcement.
6. Developing emergency response plans, and keeping them updated.
7. Establishing single points of contact, wherever possible. Ideally, these should be 24/7 contact numbers (e.g., security control centers, dispatch centers, pagers, etc.). Where companies operate in multiple states, local

## Security Guidelines for the Electricity Sector: Communications

contacts may be preferable, but single points of contact tend to ensure more timely and consistent dissemination of information within companies.

8. Previewing NERC threat guidelines with internal operating groups to ensure their understanding of the terminology and measures recommended at various threat levels. (The determination of appropriate actions to implement at each threat level depends on an individual company's assessment of its own needs, vulnerabilities and consequences, and its tolerance for risk.) The NERC/NIPC and DOE incident reporting guidelines and processes also should be reviewed with appropriate internal operating groups.
9. Notifying internal organizations that deal with release of system information (e.g., mapping, GIS information, circuit diagrams, load information, vulnerability assessments, etc.) to carefully review all requests for information to ensure the requestor is authorized and has a legitimate need to obtain that information. Wherever questionable, the request should be reviewed by the security department or other appropriate departments within the company.

### Exceptions:

### Certified Products/Tools:

### Related Documents:

- *Cyber Threat and Computer Intrusion Reporting Guidelines*, National Infrastructure Protection Center, <http://www.nipc.gov/incident/incident.htm>
- 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

# Security Guidelines for the Electricity Sector: 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