

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

NERC	Guideline
Guideline Title: Protecting Potentially Sensitive Information	Status: 1.0
Revision Date:	Effective Date: June 14, 2002

Purpose:

Critical infrastructure owners and operators should have an information security or confidentiality policy in place as an integral part of their business-level policies.

The policy should address the production, storage, transmission, and disposal of both physical and electronic information. The policy should define the hierarchical confidentiality classification framework (eg. Public, Market Participant Confidential, Company Confidential, Highly Confidential) as well as the authorization requirements and conditions to permit disclosure.

This guideline is intended to complement such a policy and should not be construed as a guide to formulating the entirety of such a policy.

Critical infrastructure owners and operators are encouraged to consider this guideline when deciding whether information should be made available to government agencies, third parties, or to the public in general. This guideline provides direction to electricity sector management and security personnel responsible for ensuring that potentially sensitive information regarding critical infrastructure is made available, only on a need-to-know basis (ie. only to the extent necessary to enable entities to execute their duties and responsibilities).

Applicability:

This guideline applies to all critical infrastructure owners and operators, and in particular, to personnel responsible for making information available to others outside their company or agency.

Guideline Statement:

Even prior to the September 11, 2001 terrorist attacks, critical infrastructure protection owners and operators expressed great concern that sensitive

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

information regarding their assets could be used by those intending to damage critical facilities, disrupt operations or harm individuals. Since September 11, that concern has required that companies and government agencies closely examine their policies regarding the release of information to outside parties.

Table of Contents:

Guideline Detail:

Applicability

Information can appear in many forms, including company reports, brochures and other promotional materials, Internet web sites, on-line documents, automated or personally conveyed information, public records, etc. In addition, each company has proprietary information, which it deems to be sensitive in nature and requires protection from inappropriate or inadvertent disclosure.

In this guideline, the term “sensitive information” refers to any information that could be used to select, or gain information about a potential critical infrastructure target by those intending to damage facilities, disrupt operations or harm individuals. The following questions will help identify potentially sensitive information.

- Has the information been cleared and authorized for appropriate release?
- Does the information contain details about critical operating facilities, systems or vulnerabilities?
- What impact could the information have if it inadvertently reached an unintended audience?
- Does the information provide details concerning physical or cyber security measures?
- Does the information contain personnel information such as biographical data, contact information, names, addresses, telephone numbers, etc.?

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

- How could someone intent on causing harm use the information to his or her advantage?
- What instructions should be given to legitimate users and recipients of sensitive information, (eg. electricity market participants, emergency response personnel, government) with regard to disseminating the information to other parties (eg. contractors, service providers, customers)?
- Could this information be dangerous if it were used in conjunction with other publicly available information?
- Could someone use the information to target personnel, facilities, or operations?
- Does the information increase the attractiveness of a critical infrastructure asset as a target?

Securing Sensitive Information

Companies should consider designating a single person or department as being responsible for reviewing all third party requests for sensitive information and, in particular, reviewing information placed in the public domain . That department will generally have to coordinate closely with the company's legal counsel.

In general, sensitive information should not be provided unless one of the following conditions is met:

1. A government agency is requesting the data and is specifically entitled to it pursuant to its regulatory or statutory authority. Although compelled to provide the information, companies should ask that the agency provide assurances that the information will be kept confidential.
2. A government agency is requesting the data without having specific regulatory authority but can provide a legitimate public safety basis for its request as well as assurances that appropriate safeguards can be provided for ensuring that the information is protected.

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

3. Third parties, such as energy companies, consultants working for such companies, developers, or others who can demonstrate a legitimate business need to have the information providing that they sign a nondisclosure agreement or other statement agreeing not to distribute the information outside their company or use it for any other purpose.

Responding to Disclosures of Sensitive Information

Companies should have in place processes to respond to disclosures of sensitive information to ensure that they are addressed promptly and appropriately. This process should include informing and involving senior management, market participants, government, regulators, law enforcement, the public and the media, as appropriate.

Training

Critical infrastructure owners and operators are encouraged to conduct ongoing employee awareness sessions to ensure that information is appropriately secured.

Examples of Potentially Sensitive Information

The following table identifies generic categories of information that, if it became available to those intending to do harm, could place critical infrastructure at greater risk from terrorist or other criminal attacks. Critical infrastructure owners and operators are encouraged to use these categories to identify potentially sensitive information relevant to their own critical assets. Such information should be limited to a need-to-know basis, and should not be made publicly available. The term “critical assets” includes the data, communications, energy and operational systems or structures necessary to maintain overall operations of the company.

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

<i>Type of Information</i>	<i>Examples</i>
Locations & Functions:	
Critical assets: function and physical location	<ul style="list-style-type: none"> • Major generating stations and switchyards • Black start facilities • Extra high voltage (>230 kV) stations • Locations and responsibilities of control and operating entities • Details of critical computer systems (eg. operational systems such as EMS, SCADA, digital control systems, their names and function, CAD/CAM facilities, network configuration and firewall schemes)
Network topology maps	<ul style="list-style-type: none"> • Ties between control areas, congestion points • GIS data of transmission networks and facilities, etc. • Hierarchical production or process control maps, charts or diagrams
Exposed/unprotected assets	<ul style="list-style-type: none"> • Bridge and over-surface assets
Unmanned assets	<ul style="list-style-type: none"> • SCADA-controlled assets • Remotely controlled assets

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

Hazardous materials	<ul style="list-style-type: none"> • Fuel, industrial chemicals or waste storage
Contingency facilities	<ul style="list-style-type: none"> • Emergency coordination centers • Emergency meeting points and stations
Assessments:	
Vulnerability or risk assessments	<ul style="list-style-type: none"> • Security assessments
Hypothetical impact assessments	<ul style="list-style-type: none"> • Hypothetical environmental impact assessments • Information that describes areas likely to be affected by a failure (eg. downstream impact of dam breach)
Drills and exercises	<ul style="list-style-type: none"> • Detailed exercise scope and objectives • Operating procedures • Findings and lessons-learned
Facility limitations	<ul style="list-style-type: none"> • Storm or other high-risk limits • Grid constraints and congestion points • Natural hazard high-risk facilities • Single contingency risks
Location/function-specific ranked data	<ul style="list-style-type: none"> • Quantitative comparisons of assets
Operations:	
Real time operations data	<ul style="list-style-type: none"> • Real time MW and flows at critical grid locations or transfer points • Hourly forebay water elevations

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

Physical and cyber security plans	<ul style="list-style-type: none"> • Facility and information technology security capabilities and procedures
Heightened risk operating procedures	<ul style="list-style-type: none"> • Critical production processes • Contingency protection measures • Special protection schemes and their operation • Emergency control actions, procedures and status when responding to events • Details of response to NERC Alert Levels
Emergency response and business continuity plans	<ul style="list-style-type: none"> • Emergency response procedures (eg. steps to be taken at a specific facility) • Facility evacuation criteria • Power system restoration plans • Contingency procedures • Minutes of meetings regarding emergency planning processes and strategies • Post-incident audits or reviews and specific action plans
Interdependencies:	
Personnel information	<ul style="list-style-type: none"> • Critical operations or emergency personnel names, addresses, telephone numbers, contact information, etc.
Energy and water sources	<ul style="list-style-type: none"> • Regular or backup energy and water sources

Security Guidelines for the Electricity Sector: Protecting Potentially Sensitive Information

Communications assets and procedures	<ul style="list-style-type: none"> • Critical communications processes and facilities • Key communications contacts and protocols
Transportation methods	<ul style="list-style-type: none"> • Key transportation routes for critical services or personnel
Key suppliers or customers	<ul style="list-style-type: none"> • Supply lines to critical facilities (military installations, hospitals, government facilities, etc.) • Critical key business process partners • Customer supply points • Number of retail customers served by a specific facility or portion of the infrastructure • Emergency and backup services • Information that could be used to identify customers and their critical infrastructure

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

Version 1.0
June 14, 2002

Security Guideline:
Protecting Potentially Sensitive Information
Page 8 of 9

Security Guidelines for the Electricity Sector: 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