

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

NERC	Guideline
Guideline Title: Threat and Incident Reporting	Version: 1.0
Revision Date:	Effective Date: June 10, 2003

Purpose:

Each organization should consider having a timely and effective reporting process for communicating security threats or incidents affecting their critical physical and cyber infrastructure. Such threats or incidents can include acts of a criminal, terrorist or cyber disruption. The purpose of this guideline is to describe this reporting process and encourage organizations to promptly report suspicious activities, threats or acts of sabotage, vandalism or terrorism. An effective reporting process will ease the burden on operations staff by enabling the appropriate involvement of the organization's physical or cyber security and emergency management personnel, as well as industry, regulatory, government and law enforcement organizations.

This security guideline does not pertain to communications and reporting procedures required for the real-time operation of electricity markets and grid operations.

While the reporting processes described are voluntary and will vary depending on the role of the organization in the electricity industry, it is the intent that such a reporting process would enable organizations to respond rapidly to the security threat or incident, and provide others outside the organization with information needed to provide assistance or take independent action.

This voluntary guideline encourages organizations to report significant security threats or incidents to the Electricity Sector – Information Sharing and Analysis Center (ESISAC). The ESISAC¹ is operated by NERC and serves the electricity sector by facilitating communications between electricity sector organizations, U.S. and Canadian federal governments and other critical infrastructure industries. The ESISAC promptly disseminates threat indications, analyses and warnings, together with its interpretations, to assist electricity sector organizations to take protective actions.

Applicability:

¹ www.esisac.com
Version 1.0
June 10, 2003

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

This guideline is intended to focus on reporting suspected or overt attacks of a physical or cyber nature with the potential to significantly affect reliable power system or market operation.

This guideline applies to entities that own or operate facilities and perform functions that are considered critical to the operation of the electricity market and power system, or critical to the overall operation of the individual organization.

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

This guideline does not supercede or replace reporting processes required for real-time power system or market operation, or as required by law. For example, organizations should have in place processes to report significant incidents affecting the bulk electric power system to their NERC reliability coordinator, who, in turn, would communicate this information with other NERC reliability coordinators across North America. The NERC reliability coordinator is responsible for ensuring the reliability of the bulk power transmission system within its reliability coordinator area, and is therefore in a position to assess the risks and call for emergency control actions such as redirecting generator dispatch, recalling transmission or generator outages, purchasing emergency energy, invoking public appeals for load reduction or implementing load shedding.

Guideline Statement:

This guideline identifies “best practices” for reporting security threats and incidents with the potential to significantly affect electricity infrastructure facilities or functions considered critical to the industry, as defined by each organization.

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

Guideline Detail:

The Need for Timely Reporting

All organizations should consider having in place processes to immediately report security threats and actual incidents that affect their operations and life safety to:

- law enforcement (e.g., local, state/provincial, FBI/RCMP);
- government agencies and regulators as is necessary or required (e.g., at the state/provincial or federal level);
- the Electricity Sector's Information Sharing and Analysis Center (ESISAC); and
- other electricity sector entities (e.g., control areas, reliability coordinators, regional transmission operators, independent system/market operators).

Some organizations are required by law to report threats or incidents within specified timeframes (e.g., DOE's Form EIA-417 Emergency Incident and Disturbance Report, NRC 10CFR73.71 and 10CFR73 Appendix G). All organizations are urged to understand these obligations and establish effective reporting processes.

Organizations should consider having in place threat and incident reporting processes that respond appropriately to the urgency of the situation. Reporting should be timely, based on the best available information, and promote the sharing of information on an actionable, need-to-know basis.

Organizations benefit from sharing threat and incident information in order to:

- promote a timely and actionable response in order to prevent the attack or mitigate the consequences on public health and safety, the environment and the economy;
- minimize negative impact on organization repair costs, revenues, productivity, customer service and public trust; and
- demonstrate diligence and due care by the organization on behalf of the electricity sector.

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

Information to be Reported

The information to be reported will vary according to the specific circumstances and availability of the information, but should include:

- date, time and location of the incident
- brief description of incident
- impact on critical infrastructure, public health and safety, environment
- expected duration of impact, or time to restore
- cause, if known
- reporting individual and organization, and contact information for follow-up
- law enforcement involvement

The Role of the ESISAC

The Electricity Sector – Information Sharing and Analysis Center (ESISAC) is operated by NERC and serves the electricity sector by facilitating communications between electricity sector organizations, the U.S. and Canadian federal governments and other critical infrastructure industries. The ESISAC promptly disseminates threat indications, analyses and warnings, together with interpretations, to assist electricity sector organizations to take protective actions.

The ESISAC facilitates communications and coordination with government agencies through the U.S. Department of Homeland Security² and Canada's Office of Critical Infrastructure Protection and Emergency Preparedness³.

Information Confidentiality

If the information provided by an organization to the ESISAC is determined by the ESISAC to warrant an industry-wide warning, then any sensitive information would be sanitized and discussed with the organization providing the information before being disseminated.

² Ref. the FBI's National Infrastructure Protection Centre at www.nipcc.gov and the Department of Energy's Office of Energy Assurance at www.oea.dis.anl.gov

³ Ref. www.ociepc-bpiepc.gc.ca

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

Organizations providing incident information to government marked “Proprietary” or “Confidential” would be protected from public disclosure through exemptions from freedom of information legislation that provide for the protection of sensitive information concerning critical cyber or physical infrastructure, specifically:

- In the U.S., Freedom of Information Act exemption B4: Trade Secrets and Proprietary Information and Section 204 of the Homeland Security Act of 2002.
- In Canada, Sections 16(2)(c) and 20(1)(b) of the Access to Information Act.

ESISAC Sharing of Information from Government Sources

The ESISAC receives sensitive-but-unclassified information from government intelligence and law enforcement sources and shares this with electricity sector organizations.

Reporting Threats and Incidents

The ESISAC has collaborated with the FBI’s National Infrastructure Protection Center (NIPC) to develop a reporting process as described in the NIPC’s Standard Operating Procedure for their Indications, Analysis and Warning (IAW) Program. It is not essential that this specific reporting process and format be followed. For example, although electronic means are in place to facilitate reporting, telephone or fax are also acceptable reporting mechanisms. This procedure is available on the ESISAC web site and provides detailed instructions for reporting security threats or incidents, including:

- Responsibilities of participating organizations, the ESISAC and government
- Timeliness requirements
- Criteria and thresholds for reporting security **incidents** known or suspected to be of a malicious origin (eg. loss of >500 MW generation for 30 minutes or longer, loss of high-voltage substations or lines, loss of firm load >200 MW for longer than 30 minutes, anomalous or uncharacteristic market or power system operation)
- Criteria and thresholds for reporting security **threats** that potentially could affect the reliable operation of the electricity market or power system (e.g., surveillance activities, intrusion attempts, security breaches)

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

Three stages of reporting provide for different information requirements at each stage of the incident. An initial Stage 1 report is intended to provide early notice that an incident meeting one or more of the criteria and thresholds has occurred. Stage 1 reports are requested within the first 60 minutes after detection of an incident, with subsequent Stage 2 reports as conditions change. A final Stage 3 report is requested when the incident has been resolved or closed.

Organizations should consider several reporting mechanisms, including, but not limited to, the following:

1. The ESISAC's Critical Infrastructure Protection Information System (CIPIS) provides a secure Internet messaging system for communication with the ESISAC, the NIPC and ESISAC participants. CIPIS users must register and be authenticated by NERC as a valid participant. Registration can be initiated at:

<http://www.nerc.net/registration/>

2. NERC reliability coordinators are required to submit reports via the Reliability Coordinator Information System (RCIS).
3. Organizations should consider establishing reporting protocols with other electricity industry participants, critically interdependent customers or service providers, industry regulators, government and law enforcement organizations.

Exceptions:

This security guideline does not pertain to communications and reporting procedures required for the real-time operation of the electricity markets and grid operations.

Related Documents:

1. Electricity Sector Critical Infrastructure Protection Communications, prepared by NERC, dated July 5, 2002.
2. Indications, Analysis and Warning Program Standard Operating Procedure (IAW SOP) prepared by the FBI's National Infrastructure Protection Center, Rev 4.0, dated February 25, 2002.
3. NERC Security Guidelines for the Electricity Sector: Threat Response, Emergency Plans, Communications, Version 1.0, dated June 14, 2002.

Version 1.0
June 10, 2003

Security Guideline:
Threat and Incident Reporting
Page 6 of 7

Security Guidelines for the Electricity Sector: Threat and Incident Reporting

Revision History:

Date	Version Number	Reason/Comments