

## Security Guideline for the Electricity Sector: Threat and Incident Reporting

### **Preamble:**

It is in the public interest for NERC to develop guidelines that are useful for improving the reliability of the bulk power system. Guidelines provide suggested guidance on a particular topic for use by bulk power system entities according to each entity's facts and circumstances and not to provide binding norms, establish mandatory reliability standards, or be used to monitor or enforce compliance.

### **Purpose:**

The criteria described in this guideline are intended to assist entities to identify and classify incidents for reporting to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). These criteria include, but are not limited to, reporting requirements imposed by some NERC standards (e.g., CIP-001, CIP-008, and EOP-004) and the U.S. Department of Energy (DOE) (OE-417) and requests for voluntary reporting from the U.S. Department of Homeland Security (DHS) and Public Safety Canada/Royal Canadian Mounted Police (RCMP) (a cross-reference is included as Appendix A).

This guideline also identifies available reporting mechanisms.

Operated by NERC, the ES-ISAC serves the electricity sector by facilitating communications between electricity sector entities, U.S. and Canadian federal governments, and other critical infrastructure sectors. The ES-ISAC promptly disseminates threat indications, analyses and warnings to assist electricity sector entities to evaluate the situation and take appropriate actions.

### **Scope of Application:**

This guideline focuses on incidents that have adversely affected or have the potential to adversely affect the reliability of the bulk power system. It is intended for use by owners, operators, and users of the bulk power system.

The criteria in this guideline are not requirements, nor should they be construed as such. This guideline does not supersede reporting required for power system operation or as required by law.

This document replaces the DHS/ES ISAC Indications, Analysis, and Warning Program Standard Operating Procedure (IAW SOP), dated August 19, 2005. It also replaces the Threat and Incident Reporting Guideline, dated June 2003.

### **Guideline Details:**

The following list describes incidents that entities should consider reporting to the ES-ISAC. Entities can also consider submitting reports to their respective regional entity.

While there are many observable events on the bulk power system, not all need to be reported. It is up to each entity to classify and identify incidents that are most likely to have a detrimental effect on the reliability of the bulk power system should they occur and to develop procedures to report them to the ES-ISAC. This guideline contains criteria and thresholds to assist entities in these activities. For reference, Appendix A is a summary of these criteria in tabular form.

Refer to the reference documents for detailed explanations of reporting definitions and time frames.

Entities are encouraged to report any incident whose cause is known to be malicious, is suspected of being malicious, or is unknown. Moreover, entities are encouraged to report incidents as soon as practical.

### **Event category: EMERGENCY ACTIONS**

1. **Public Appeal** — An official request by a utility, U.S. regulatory agency, or U.S. government entity that the public reduce its consumption of electricity.

Report when: an appeal has been issued.

Report within: 1 hour of the appeal being issued.

2. **Voltage Reduction** — An entity intentionally lowers the voltage on its system in order to reduce demand.

Report when: operator-initiated reductions of 3 percent or more are applied system wide.

Report within: 1 hour after the reduction was initiated.

3. **Firm Load Shedding** — The intentional outage of customer load in significant quantities either through automatic or operator-initiated actions to protect the bulk power system.

Report when: anticipated or actual disconnection of 100 MW or more occurs.

Report within: 1 hour of the start of the shedding incident.

4. Relocation of Control Center Operations — Transfer of operational control to an alternate site or a return of control to a primary control center.

Report when: the need to transfer control is out of operational necessity, rather than for the purposes of testing or training.

Report within: 2 hours of the start of relocation.

**Event category: SYSTEM DISTURBANCES**

1. Loss of Firm Load — The unintentional outage of firm customer load, including distribution load.

Report when:

- 300 MW or more is lost for more than 15 minutes, or,
- More than 50,000 customers or more are affected for an hour or more.

Report within: 1 hour (300 MW) or 6 hours (50,000 customers).

2. Forced Outage — A loss of or required removal from service availability of a generating unit, transmission line, or other equipment due to unanticipated reasons.

Report when:

- the forced outage is due to an actual or suspected physical attack on a generation or transmission asset, or
- the forced outage of a generation asset 500 MW or above is due to unknown causes, or
- a forced outage of generation of more than 2,000 MW occurs in the Eastern or Western Interconnection, or
- a forced outage of generation of more than 1,000 MW occurs in ERCOT, or
- the forced outage causes the loss of a transmission facility, significantly affecting the integrity of interconnected system operations, or

- an analysis of the outage results in any of the following actions:
  - a. modification of operating procedures.
  - b. modification of equipment (e.g., control systems or special protection systems) to prevent reoccurrence of the event.
  - c. identification of valuable lessons learned.
  - d. identification of non-compliance with NERC standards or policies.
  - e. identification of a disturbance that is beyond recognized criteria, i.e., three-phase fault with breaker failure, etc.

Report within: 24 hours of outage or upon taking action as a result of outage analysis.

3. Frequency Excursions — A significant change in the interconnection frequency that occurs suddenly or over a period of time.

Report when: the excursion is below the underfrequency load shed point for firm loads.

Report within: 24 hours of the excursion.

4. Voltage Excursions or Collapse — A significant change in the voltage that occurs suddenly or over a period of time.

Report when: excursion is +/- 10% of nominal voltage or is below undervoltage load shed point.

Report within: 24 hours of excursion.

5. Islanding or Separation — Part or parts of an interconnection remain(s) in operation following the separation of normally interconnected areas.

Report when: islanding or separation occurs.

Report within: 1 hour of occurrence.

6. Complete System Failure (Blackout) — Complete operational failure or shutdown of an entity's transmission or distribution electrical system or both.

Report when: transmission or distribution electrical system experiences a complete operational failure or shutdown.

Report within: 1 hour of failure.

**Event category: SABOTAGE/TAMPERING/VANDALISM – Physical or Cyber**

1. Security Breaches:

- a. Physical Perimeter Compromise — Unauthorized access of a person or a device through, circumventing, or damaging the physical perimeter or security systems protecting the physical perimeter.

Report when: unauthorized physical access to facilities, systems, or equipment (such as critical assets or critical cyber assets) that could impact the reliable operation of the bulk power system; or, intentional damage to security systems that protect the physical perimeter.

Report within: 1 hour of detection.

- b. Cyber Perimeter Compromise — Unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device.

Report when: unauthorized electronic access to cyber assets whose impairment could impact the reliability of the bulk power system occurs.

Report within: 1 hour of detection.

- c. Information Theft or Loss — Unauthorized removal of an item of value.

Report when: sensitive information, such as that required to be protected pursuant to NERC Standard CIP 003, is lost or is removed without authorization.

Report within: 48 hours of discovery of theft or loss.

- d. Unauthorized modification — Unauthorized addition or modification of software or data associated with the proper operation of cyber assets.

Report when: malicious software or data modification is discovered on a cyber asset or assets that may impact the reliability of the bulk power system.

Report within: 4 hours of detection.

2. Suspected Activities:

- a. Attempted Physical Intrusion — A detected effort to gain unauthorized access of a person or a device through the physical perimeter but without obvious success.

Report when: attempt to gain unauthorized physical access to facilities, systems, or equipment (such as critical assets or critical cyber assets) that could impact the reliable operation of the bulk power system is targeted, focused, or repetitive.

Report within: 1 hour of detection.

- b. Attempted Cyber Intrusion — A detected effort to gain unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device but without obvious success.

Report when: attempt to gain unauthorized electronic access to cyber assets (such as critical cyber assets) whose impairment could impact bulk power system reliability is targeted, focused, or repetitive.

Report within: 1 hour of detection.

3. Surveillance Activities – Intelligence Gathering:

- a. Social Engineering — The attempt by an unauthorized person to manipulate people into performing actions or divulging information.

Report when: suspected or actual instances of social engineering occur.

Report within: 8 hours of recognition.

- b. Photography — Taking still or moving pictures.

Report when: incident of photo taking is suspicious.

Report within: 8 hours.

- c. Observation — Showing unusual interest in a facility; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.

Report when: activity is suspicious or unauthorized.

Report within: 8 hours.

- d. Flyover — Flying an aircraft over a facility; this includes any type of flying vehicle including an unmanned aerial vehicle (UAV) loitering over a site.

Report when: activity is suspicious or unauthorized.

Report within: 8 hours.

#### 4. Threats:

- a. Expressed Threat — Communicating a threat.

Report when: threatened action has the potential to damage or compromise a facility or personnel.

Report within: 1 hour of receipt of threat.

- b. Weapons Discovery — Discovery of explosives.

Report when: explosives are discovered at or near a facility.

Report within: 1 hour of detection.

Attack (Physical or Cyber or Communication) — Attack via physical, cyber, or communications means.

Report when: suspected or actual attacks against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel occur.

Report within: 1 hour of an actual attack.  
6 hours of a suspected attack.

**Event category: EQUIPMENT AND /OR SYSTEMS FAILURE**

1. Failure or Compromise of Computer Software or Hardware Used for Control, Monitoring or Alarming — Failure or malfunction of any critical reliability tool or system, or components thereof, such as EMS, SCADA, or other critical cyber assets as identified pursuant to NERC Standard CIP-002.

Report when: the unplanned loss or malfunction may result in actual or potential risk to the bulk power system and lasts 30 minutes or longer.

Report within: 1 hour of loss or malfunction.

2. Communication Systems Failure, Impairment, or Compromise — Failure, degradation of functionality, or unauthorized access or use of facilities used for the exchange of voice or data.

Report when:

- the incident disrupts the monitoring or operation of the bulk power system, or
- the incident involves unauthorized access to or use of systems.

Report within: 6 hours

**Event category: OTHER**

1. Fuel Supply Problems — Problem with the fuel supply to a generating unit or station. Problems may be due to transportation, supply, delivery, or quality of the fuel.

Report when: fuel supply problems could impact electric power system reliability or adequacy; or, fuel inventories or hydro storage levels are 50% of normal or less.

Report within: 6 hours of the recognition that a problem exists.

Loss of Off-site Power at Nuclear Unit — Degradation of voltage below minimum requirements of the electric power supply provided from the transmission system to the nuclear power plant distribution system as required per the nuclear power plant license.

Report when: voltage degrades beyond required limits.

Report within: 1 hour.

### **Information to Report**

The amount of information to report for each incident should include the following:

- reporting individual, entity name, and contact information for follow-up;
- date, time and location (NERC region, state/province, city) of the incident;
- brief description of incident, including affected transmission and generation facilities, load loss, generation loss, reactive and voltage impacts and approximate number of customers and their locations as appropriate;
- impact on critical infrastructure, public health and safety, environment;
- expected duration of impact, or time to restore;
- cause, if known; and
- law enforcement involvement.

To facilitate reporting, the ES-ISAC has developed an incident report form, which is available for download at [www.esisac.com](http://www.esisac.com). This form has been incorporated into electronic reporting mechanisms noted below. For incidents that meet the OE-417 or EOP-004 reporting requirements, entities may submit those forms to the ES-ISAC.

### **Reporting Timeliness**

Entities should develop processes to ensure timely reporting of incidents to the ES-ISAC. These processes also should address timely reporting to others with a need-to-know, including:

- 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);
- other electricity sector entities (e.g., balancing authorities, reliability coordinators, regional transmission operators, and independent system/market operators); and,
- critically interdependent customers or service providers.

Reporting should be based on the best available information, and promote the sharing of information on an actionable, need-to-know basis. Entities are encouraged to report incidents as soon as practical.

Some entities are required by law to report incidents within specified time frames (e.g., DOE's Form OE-417 Emergency Incident and Disturbance Report). It is incumbent upon all entities to understand their reporting obligations.

### **Reporting Mechanisms**

The following list provides information about various tools that entities may opt to use to report events and incidents to the ES-ISAC and other information sharing partners. Entities may choose to use one or more tools depending on the incident to be reported.

1. Critical Infrastructure Protection Information System (CIPIS)  
Provides a secure Internet messaging system for communication with the ES-ISAC, DHS, Public Safety Canada, and electricity sector participants. Access to CIPIS is restricted to authorized electricity sector participants. Registration instructions are available at [www.esisac.com](http://www.esisac.com).
2. Reliability Coordinator Information System (RCIS)  
NERC reliability coordinators have the option to use this secure messaging system for event and incident reporting. Use of RCIS is limited to reliability coordinators.
3. Telephone, fax, or email  
Phone: 609-452-1422 (24x7)  
Fax: 609-452-9550 (normal business hours)  
E-mail: [esisac@nerc.com](mailto:esisac@nerc.com) (anytime)

### **Information Dissemination and Confidentiality:**

Upon approval of the submitting entity, incident reports received by the ES-ISAC may be transmitted to government agencies in the United States and Canada, to other electric sector participants, and to other critical infrastructure sectors on a confidential and need-to-know basis.

The ES-ISAC follows established procedures for protecting confidential information prior to sharing with others.

Incident reports containing confidential information shared voluntarily with

government agencies are protected from public disclosure per the following legislation and regulations.

- In the United States:
  - Critical Infrastructure Information Act of 2002 (CII Act)
  - DHS Protected Critical Infrastructure Information (PCII) regulations
  - FERC Critical Energy Infrastructure Information (CEII), Order No. 683, September 21, 2006
  - 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
  - Emergency Management Act (bill C12)

**Related Documents and Links:**

1. NERC Reliability Standard CIP-001-1, [Sabotage Reporting](#), January 1, 2007.
2. NERC Reliability Standard CIP-008-1, [Incident Reporting and Response Planning](#), June 1, 2006.
3. NERC Reliability Standard EOP-004-1, [Disturbance Reporting](#), January 1, 2007.
4. U.S. Department of Energy, Office of Energy Assurance, [OE-417 — Electric Emergency Incident and Disturbance Report](#), April 2007.

**Revision History:**

Date	Version Number	Reason/Comments
7/29/08		Additional citation under the Information Dissemination and Confidentiality section.

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
<b>EMERGENCY ACTIONS</b>					
	Public Appeals	An official utility, regulatory agency, or government request that the public reduce its consumption of electricity.	An appeal has been issued.	1 hour	EOP-004, Attachment 2, Table 1, Incident #4
	Voltage Reduction	An entity intentionally lowers the voltage on its system in order to reduce demand.	Operator-initiated reduction of 3 percent or more is applied system wide.	1 hour	EOP-004, Attachment 2, Table 1, Incident #3
	Firm Load Shedding	The intentional outage of customer load in significant quantities either through automatic or operator-initiated actions to protect the bulk power system.	Anticipated or actual disconnection of 100 MW or more occurs.	1 hour	EOP-004, Attachment 2, Table 1, Incident #2
	Relocation of Control Center Operations	Transfer of operational control to an alternative site or a return of control to a primary control center.	The transfer of control, due to operational necessity rather than testing or training, has started.	2 hours	ES-ISAC
<b>SYSTEM DISTURBANCES</b>					
	Loss of Firm Load	The unintentional outage of firm customer load, including distribution load.	300 MW or more is lost for more than 15 minutes from a single incident.	1 hour	EOP-004, Attachment 2, Table 1, Incident #1
			More than 50,000 customers are affected for an hour or more.	6 hours	

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
	Forced Outage	A loss of or required removal from service availability of a generating unit, transmission line, or other equipment due to unanticipated reasons.	<p><b>Generation:</b>            500 MW or more is affected due to unknown causes.             2,000 MW or more is affected in the Eastern Interconnection or in WECC or 1,000 MW or more is affected in ERCOT regardless of the actual or suspected cause.</p> <p><b>Transmission:</b>            Loss of a facility that significantly affects the integrity of bulk power system operations.</p> <p><b>Other:</b>            Analysis of the outage leads to one or more of the following actions:            a. modification of operating procedures.            b. modification of equipment (e.g., control systems or special protection systems) to prevent reoccurrence of the event.            c. identification of valuable lessons learned.            d. identification of non-compliance with NERC standards or policies.            e. identification of a disturbance that is beyond recognized criteria, i.e., three-phase fault with breaker failure, etc.</p>	24 hours	<p>ES-ISAC</p> <p>EOP-004, Attachment 1, Item 3</p> <p>EOP-004, Attachment 1, Item 1</p> <p>EOP-004, Attachment 1, Item 1</p>
	Frequency Excursions	A significant change in the interconnection frequency that occurs suddenly or over a period of time.	Excursion is below underfrequency load shed point for firm loads.	24 hours	EOP-004, Attachment 1, Item 1f

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
	Voltage Excursions/ Collapse	A significant change in the voltage that occurs suddenly or over a period of time.	Excursion is +/- 10% of nominal voltage or is below undervoltage load shed point.	24 hours	EOP-004, Attachment 1, Item 1f and Item 6
	Islanding or Separation	Part or parts of an interconnection remain(s) in operation following the separation of normally interconnected areas.	Islanding or separation occurs.	1 hour	EOP-004, Attachment 1, Item 2
	Complete System Failure (Blackout)	Complete operational failure or shutdown of an entity's transmission or distribution electrical system or both.	A complete operational failure or shutdown of transmission or distribution electrical system or both occurs.	1 hour	EOP-004, Attachment 2, Table 1, Incident #9
<b>SABOTAGE/TAMPERING/VANDALISM (STV) – Physical or Cyber</b>					
	<b>Security Breaches:</b>				
	Physical Perimeter Compromise	Unauthorized access of a person or a device through, circumventing, or damaging the physical perimeter, or security systems protecting the physical perimeter.	Unauthorized physical access to facilities, systems, or equipment (such as critical assets or critical cyber assets) that could impact the reliable operation of the bulk electric system; or, intentional damage to security systems that protect the physical perimeter.	1 hour of detection	EOP-004, Attachment 2, Table 1, Incident #5
	Cyber Perimeter Compromise	Unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device.	Unauthorized electronic access to cyber assets whose impairment could impact the reliability of the bulk power system is unauthorized.	1 hour of detection	EOP-004, Attachment 2, Table 1, Incident #6

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
	Information Theft or Loss	Unauthorized removal or loss of sensitive information.	Sensitive information, such as that required to be protected pursuant to NERC Standard CIP-003 is lost or is removed without authorization.	48 hours of detection	ES-ISAC
	Unauthorized Modification	Unauthorized addition or modification of software or data associated with the proper operation of cyber assets.	Malicious software or data modification is discovered on a cyber asset or assets that may impact the reliability of the bulk power system.	4 hours of detection	ES-ISAC
Suspected Activities:					
	Attempted Physical Intrusion	A detected effort to gain unauthorized access of a person or a device through the physical perimeter but without obvious success.	Attempt to gain unauthorized physical access to facilities, systems, or equipment (such as critical assets or critical cyber assets) that could impact the reliable operation of the bulk power system is targeted, focused, or repetitive.	6 hours upon detection	EOP-004, Attachment 2, Table 1, Incident #5
	Attempted Cyber Intrusion	A detected effort to gain unauthorized ingress or egress through the electronic perimeter or into an electronic perimeter device but without obvious success.	Attempt to gain unauthorized electronic access to cyber assets (such as critical cyber assets) whose impairment could impact bulk power system reliability is targeted, focused, or repetitive.	6 hours upon detection	EOP-004, Attachment 2, Table 1, Incident #6
Surveillance Activities – Intelligence Gathering:					
	Social Engineering	The attempt by an unauthorized person to manipulate people into performing actions or divulging information.	Suspected or actual instance occurs.	8 hours of recognition	ES-ISAC
	Photography	Taking still or moving pictures.	A suspicious incident occurs.	8 hours	ES-ISAC
	Observation	Showing unusual interest in a facility; for example, observing it through binoculars, taking notes, drawing maps, or drawing structures of the facility.	Activity is suspicious or unauthorized.	8 hours	ES-ISAC

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
	Flyover	Flying an aircraft over a facility; this includes any type of flying vehicle including an unmanned aerial vehicle (UAV) loitering over a site.	A suspicious or unauthorized incident occurs.	8 hours	ES-ISAC
<b>Threats:</b>					
	Expressed Threat	Communicating a threat.	Threatened action has the potential to damage or compromise a facility or personnel.	1 hour	ES-ISAC
	Weapons Discovery	Discovery of explosives.	Discovery occurs at or near a facility.	1 hour	ES-ISAC
<b>Attacks:</b>					
	Actual Attack (Physical or Cyber or Communication)	Attack via physical, cyber, or communications means.	An actual attack against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel occurs.	1 hour	EOP-004, Attachment 2, Table 1, Incident #5 & 6
	Attempted Attack (Physical or Cyber or Communication)	Attack via physical, cyber, or communications means.	A suspected attack against generation, transmission, or company-owned or operated communication facilities, cyber assets, or personnel occurs.	6 hours	EOP-004, Attachment 2, Table 1, Incident #5 & 6

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
<b>EQUIPMENT AND/OR SYSTEMS FAILURE</b>					
	Failure or Compromise of Computer Software or Hardware Used for Control, Monitoring or Alarming.	Failure or malfunction of any critical reliability tool or system, or components thereof, such as EMS, SCADA, or other critical cyber asset as identified pursuant to NERC Standard CIP-002.	Unplanned loss or malfunction lasting 30 minutes or longer that may result in actual or potential risk to the bulk power system.	1 hour	ES ISAC
	Communication Systems Failure, Impairment, or Compromise	Failure, degradation of functionality, or unauthorized access or use of facilities used for the exchange of voice or data.	Disrupts the monitoring or operations of bulk power system.  Unauthorized access to or use of systems whether or not the bulk power system is affected.	6 hours	OE-417 - Schedule 1, Item 10
<b>OTHER</b>					
	Fuel Supply Problems	Problem with the fuel supply to a generating unit or station. Problems may be due to transportation, supply, delivery, or quality of the fuel.	Fuel supply problem could impact electric power system reliability or adequacy or fuel inventories or hydro storage levels are 50% of normal or less.	6 hours of the recognition of a problem	EOP-004, Attachment 2, Table 1, Incident #7
	Loss of Off-site Power at Nuclear Unit	Degradation of voltage below minimum requirements of the electric power supply provided from the transmission system to the nuclear power plant distribution system as required per the nuclear power plant license.	Voltage degrades beyond required limits.	1 hour	ES-ISAC

\* This cross-reference is provided for convenience. It is not intended to be inclusive. Entities must understand and meet their required reporting obligations.

**NERC Guideline: Threat and Incident Reporting**

**Attachment A: Reporting Cross-Reference Matrix\***

Category	Sub-category	Event Definition	Report When:	Report Within:	Reference
----------	--------------	------------------	--------------	----------------	-----------

**Reporting Mechanisms:**

The following list provides information about various tools that entities may opt to use to report events and incidents to the ES-ISAC and other information sharing partners. Entities may choose to use one or more tools depending on the incident to be reported.

**1. Critical Infrastructure Protection Information System (CIPIS)**

Provides a secure Internet messaging system for communication with the ES-ISAC, Department of Homeland Security, Public Safety Canada, and electricity sector participants. Access to CIPIS is restricted to authorized electricity sector participants. Registration instructions are available at [www.esisac.com](http://www.esisac.com).

**2. Reliability Coordinator Information System (RCIS)**

NERC reliability coordinators have the option to use this secure messaging system for event and incident reporting. Use of RCIS is limited to reliability coordinators.

**3. Telephone, fax or email**

Phone: 609-452-1422 (24x7)

Fax: 609-452-9550 (business hours)

Email: [esisac@nerc.com](mailto:esisac@nerc.com) (anytime)