Quick Takes

Market Participant Event Reporting

Issue 25 **March 25, 2013**

Introduction

This edition of *Quick Takes* describes the mandatory requirements and best practices for market participants to report events affecting, or having the potential to affect, the Bulk Electric System (BES), including:

- Security-related events such as:
  - Cyber-security events.
  - Physical-security events.
- All other disturbances.

The reporting details described in this document apply to all events, including those that are suspected or determined to be caused by sabotage.

Market participants can use this document to determine when an event should be reported to the IESO (for more details on event reporting to the IESO, refer to MDP_PRO_0040 – *Market Manual 7: System Operations, Part 7.1: System Operating Procedures*, section 3: *Communication Protocol*).

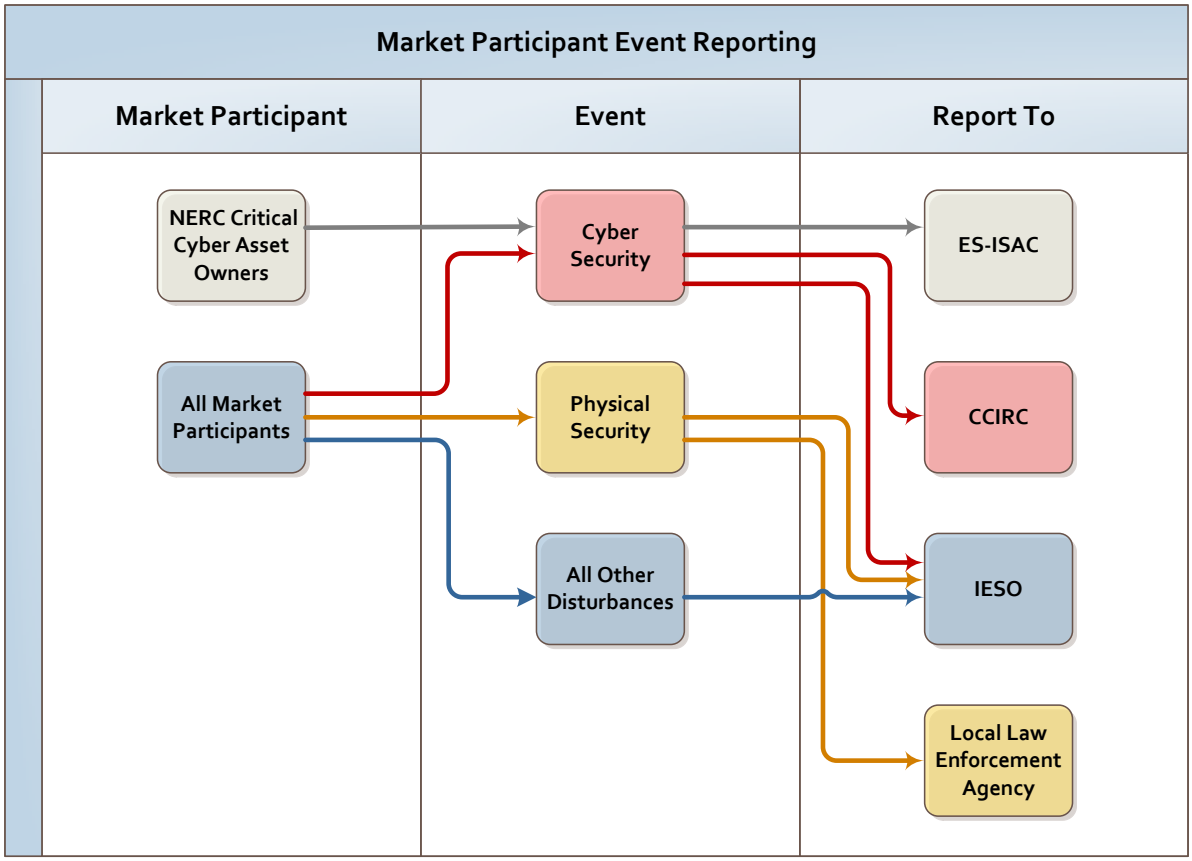
Background

There are many events that impact, or have the potential to impact, the reliability of the IESO-Controlled Grid (ICG). These can include power system events resulting from equipment failure, human error, equipment misoperation, and severe weather, as well as intentional acts such as physical sabotage and cyber-attack. In addition to mandatory reporting obligations that many market participants must follow, it is important that the IESO is notified of these events so that we can mitigate their impact on the operation of the power system. Timely information sharing is critical in this regard.

Many of the reporting requirements around system disturbances are well-established and understood by market participants; however, this is not necessarily the case for security-related incidents. In 2009, Canada's "National Strategy for Critical Infrastructure" was developed and includes the "Share and Protect Information" program. Through this program, specific initiatives were undertaken by the Government of Canada to partner with the private sector in order to facilitate more effective sharing of security-related information. As a result, the need to report both physical and cyber-security events has expanded to include events that affect, as well as those that have the potential to affect, the reliability of the ICG.

In support of this, security-related events should be reported as follows (refer to the *Report Submission* section at the end of this document for more detailed information):

- Cyber-security events should be reported to the Canadian Cyber Incident Response Centre (CCIRC).
- Physical-security events can be reported to your local law enforcement agency.
- Both physical and cyber-security events should be reported to the IESO.
- Market participants with NERC critical cyber assets (as defined under CIP-002-3) should report cyber-security incidents to NERC's Electricity Sector Information Sharing and Analysis Center (ES-ISAC).



We have prepared this quick-reference because we need market participants to be able to identify and supply event information in a prompt manner. We have attempted to address both mandatory requirements and best practices for reporting all system events in order to maintain the integrity of the ICG. This document is not intended to replace market participant reporting requirements as described in the applicable NERC reliability standards listed below.

NERC Standard ID	Title
CIP-001-2a	Sabotage Reporting
CIP-008-3	Cyber Security – Incident Reporting and Response Planning

As the Reliability Coordinator, Balancing Authority, and Transmission Operator for Ontario, the IESO is also responsible for reporting system disturbance events to NERC (and NPCC) on behalf of the province to comply with various other standards and requirements (refer to the resource material listed at the end of this document for a complete list of applicable NERC reliability standards). For this reason, it is imperative that we receive timely reports from all Ontario market participants relating to any of the events described in this document.

Market participants who have designated critical cyber assets should report cyber-security incidents to NERC's ES-ISAC even if they are not NERC-registered entities.

The IESO Market Rules, Chapter 5, section 14: *Information and Reporting Requirements* states that:

- 14.1.4 - Each market participant shall provide to the IESO such data as may be required by the IESO to enable it to satisfy a request by a standards authority.
- 14.1.5 - The IESO shall file such reports including, but not limited to, disturbance reports, and participate in such discussions as may be required by relevant standards authorities. Each market participant shall provide to the IESO such information and reports as may be required by the IESO to facilitate preparation by the IESO of such disturbance reports.

Reporting Requirements

Timely communication between market participants and the IESO is vital for the secure and reliable operation of the ICG. The table below summarizes events deemed reportable to the IESO ('X' indicates a reportable event for any given participant). Many of these events must be reported to NERC within 60 minutes of the start of the event. For this reason, these events must be reported to the IESO without delay.

Reportable Event	Participant Category					
	Transmitters	Generators	Distributors	Embedded Market Participants	Connected Wholesale Customers	Other Market Participants
Automatic operations of all circuit breakers that form part of the ICG.	X					
Operation of power system auxiliaries such as special protection systems and under-frequency protection.	X	X	X		X	
Degradation of auxiliary equipment, control equipment, or staffing that reduces security of the ICG.	X	X				
Degradation of switchyard auxiliaries, such as air compressors, that could affect the reliability of the ICG.	X	X				
Any indication of a power system event, such as, oscillations of real or reactive power, voltage declines of 10% or greater, operation of disturbance recorders, etc.	X					
Loss of reactive power capability or resources of 15 MVAR or greater for areas electrically South of Essa in Barrie, or 10 MVAR or greater for areas electrically North of Essa in Barrie.	X					
Restrictions on equipment in the ICG.	X	X	X			

Reportable Event	Participant Category					
	Transmitters	Generators	Distributors	Embedded Market Participants	Connected Wholesale Customers	Other Market Participants
Security-related events affecting or having the potential to affect the ICG, including: • Cyber-security events. • Physical-security events.	X	X	X	X	X	
Disturbances or unusual occurrences that jeopardize the operation of the BES, or result in system equipment damage or customer interruptions.	X	X	X	X	X	
Unscheduled step changes in a generation unit's output of greater than 50 MW or 10 MVAR.		X				
De-ratings in a generation unit's output of greater than 50 MW or 10 MVAR.		X				
Automatic removal from service of generation, or generation facilities of 20 MW nominal capacity or greater.		X				
Unavailability of any generation units that are included in operating reserve.		X				
Frequency outside the range of 59.8 Hz to 60.2 Hz.	X	X	X			
Upon request, the unit status information of the Available But Not Operating (ABNO) units.		X				

Reportable Event	Participant Category					
	Transmitters	Generators	Distributors	Embedded Market Participants	Connected Wholesale Customers	Other Market Participants
Any automatic loss or forced manual interruption of load greater than 100 MW, or 50 MW electrically north of Essa TS in Barrie.	X		X		X	
Automatic removal from service of reactive capability of 15 MVAR or greater that are dispatchable by the IESO for areas electrically south of Essa in Barrie, or 10 MVAR or greater that are dispatchable by the IESO for areas electrically north of Essa in Barrie.	X		X		X	
Degradation of power system auxiliaries that reduces security of the ICG.			X		X	
Loss of any internal distribution line(s) that affects the output of an embedded generation facility of 20 MW or greater in nominal capacity or dispatchable load.			X		X	
Any operating restrictions or removal from service of equipment that could affect the reliability of the ICG.	X		X		X	
Any loss of load greater than 100 MW, or 50 MW electrically north of Essa TS in Barrie, or generation in excess of 20 MW.	X			X		

Reportable Event	Participant Category					
	Transmitters	Generators	Distributors	Embedded Market Participants	Connected Wholesale Customers	Other Market Participants
Any commercially induced load curtailments (e.g., water heaters) that they initiate beyond the scope of such advisement that are contained within the market rules. Confirmations of the load curtailment and amounts, cessation of load curtailment requests, and load restoration times will also be communicated.						X
Any extraneous factors that may affect the operation of the ICG, such as (any change in such conditions shall likewise be communicated):						
• Inclement weather.	X	X	X		X	
• Forest fires.	X	X	X		X	
• Directions from civil authorities (i.e., fire and police).	X	X	X		X	
• Environmental factors such as air pollution advisories/control orders.		X				
• Depleted fuel inventories.		X				
• Abnormal water flow conditions.		X				
• Loss of water control and/or dam safety concerns.		X				

Note: Auxiliary equipment includes:

- All protection systems (including line, transformer, overvoltage, overcurrent, and high resistance open phase).
- All communications facilities associated with protections.
- All dynamic control systems: AVRs, power system stabilisers, other excitation system components.
- All special protection systems.
- All under-frequency load shedding relays.
- All automatic re-closure schemes.
- All automatic tap changer controls on 500 kV/230 kV, 500 kV/115 kV, and 230 kV/115 kV autotransformers.
- All voltage reduction facilities that are used for demand control.
- Ferro-resonance protection schemes.
- All voice communications facilities that are required by the Market Rules.
- Automatic generation control facilities.
- Supervisory Control and Data Acquisition (SCADA) facilities.

Additional Requirements

In addition to the requirements listed above, the following conditions also apply:

- Generators who have operating control of portions of the ICG shall abide by any communications requirements specified for transmitters.
- Distributors that control portions of the ICG shall abide by any communications requirements that apply to transmitters.
- Embedded market participants that control portions of the ICG shall abide by any communications requirements that apply to distributors.
- Connected wholesale customers that control portions of the ICG shall abide by any communications requirements that apply to transmitters.

Report Submission

To report events related to cyber or physical security to the IESO:

- E-mail: security.events@ieso.ca

To report cyber-security events to CCIRC:

- Email: cyberdo@ps-sp.gc.ca

To report cyber-security events to NERC's ES-ISAC:

- Report an Incident

Reporting Timeline

Please refer to the appropriate NERC reliability standard for specific reporting timeline requirements. In all cases, the prompt reporting of events described in this document is essential for the secure and reliable operation of the ICG.

Summary

This document is intended as a quick-reference guide to assist market participants in understanding the events that they need to report. For more detailed information, please refer to the resource material listed below.

Additional Information

- Market Rules, Chapter 5, section 14: *Information and Reporting Requirements*
- MDP_PRO_0040 – *Market Manual 7: System Operations, Part 7.1: System Operating Procedures*, section 3: *Communication Protocol*
- NERC Reliability Standard CIP-001-2a - *Sabotage Reporting*
- NERC Reliability Standard CIP-002-3 - *Cyber Security — Critical Cyber Asset Identification*
- NERC Reliability Standard CIP-008-3 - *Cyber Security – Incident Reporting and Response Planning*
- NERC Reliability Standard EOP-002-3.1 - *Capacity and Energy Emergencies*
- NERC Reliability Standard EOP-004-1 - *Disturbance Reporting*
- NERC Reliability Standard IRO-006-5 - *Reliability Coordination - Transmission Loading Relief*
- NERC Reliability Standard TOP-007-0 - *Reporting SOL and IROL Violations*
- Canada's National Strategy for Critical Infrastructure