



MARKET ASSESSMENT & COMPLIANCE DIVISION SANCTIONING GUIDELINES

Effective date: September 10, 2008

(Page intentionally left blank)

Table of Contents

INTRODUCTION	1
SCOPE	2
OVERVIEW	3
Steps	3
DESCRIPTION OF STEPS	3
DESCRIPTION OF PRINCIPLES	5
DUE PROCESS ADDITIONS.....	12

List of Tables

TABLE 1: Section 6.6.6B Penalty Matrix.....	4
TABLE 2: Impact Levels	6
TABLE 3: Non-Compliance Level Criteria:.....	6

Guidelines for Extraordinary Financial Penalties Under the Ontario Electricity Market Rules

Financial Penalties Up to \$1 million (Chapter 3, section 6.6.6A and 6.6.6B)

INTRODUCTION

Section 6 of Chapter 3¹ of the Ontario Electricity Market Rules (“market rules” or “rules”) describes the framework for the enforcement of compliance with the market rules, including the circumstances under which the Independent Electricity System Operator (“IESO”) may impose sanctions, including financial penalties, for breaches of the rules. Section 6.2.7.5 specifies that financial penalties may only be imposed if:

“...the *IESO* is satisfied that the breach could have been avoided by the exercise of due diligence by the market participant or that the *market participant* acted intentionally;”

Sections 6.6.1 – 6.6.7 specify the circumstances under which a financial penalty may be fixed within four penalty ranges: 1) up to \$2,000, 2) up to \$4,000, 3) up to \$6,000, and 4) up to \$10,000.

Section 6.6.6A allows the IESO to impose a financial penalty in excess of these amounts, up to \$1 million per occurrence.

The purpose of these guidelines is to describe how the enforcement arm of the IESO, the Market Assessment and Compliance Division (“MACD”), will fix the amount of a financial penalty for matters falling under section 6.6.6A which reads as follows:

“The *IESO* may impose on a *market participant* a financial penalty in excess of the amount otherwise provided for in section 6.6.6 and no greater than \$1,000,000 per occurrence, where:

6.6.13.1 the *market participant* has breached a *market rule* while a declaration that the *IESO-controlled grid* is in an *emergency operating state* or a *high-risk operating state* was in effect;

6.6.13.2 the *market participant* breached a *market rule* while a declaration that *market operations* have been suspended was in effect;

¹ All section references in this document refer to Chapter 3 of the Market Rules

Sanctioning Guidelines

6.6.13.3 the *IESO Board* determines that the impact of the *market participant's* breach of a *market rule* on either the *IESO-administered markets* or the *reliability* of the *integrated power system* is particularly severe; or

6.6.13.4 the rate of recurrence of non-compliance by the *market participant* with the *market rules* is of such frequency or duration as to warrant the imposition of a higher financial penalty."

The central feature of the guidelines is a table or matrix ('Section 6.6.6B Penalty Matrix') identifying dollar ranges from \$2,000 to \$1 million, according to the assessment of the impact ('impact level') of the breach, as well as its severity and the record of non-compliance ('breach history') of the party, and any adjustments. A final penalty amount within the selected range is determined based on an assessment of a set of factors, including those that may be aggravating or mitigating. The underlying principle of the guidelines is that their application results in a financial penalty that bears a direct relationship to the seriousness of the breach.

In keeping with well-established principles of enforcement and adjudication, the guidelines provide a measure of the likely size of a financial penalty for a given breach, but they are not a mathematical formula or algorithm. The final penalty amount will always be an exercise of judgement based on an assessment of the facts of the particular case.

To ensure that the party being assessed a financial penalty under section 6.6.6A has an adequate opportunity to bring forward relevant information and evidence, the guidelines also specify that MACD's review provides the party with an opportunity to meet and provide written comments on MACD's preliminary assessment. This mirrors the procedures in the rules for determining whether a breach of the rules has occurred.

SCOPE

These guidelines come into play after a breach has been determined. The finding of a breach and the fixing of a financial penalty in the range allowed for under section 6.6.6A are separate matters. These guidelines address the latter.

These guidelines address the fixing of a financial penalty in the range allowed for under section 6.6.6A. They do not speak to whether a breach qualifies for consideration to be assessed a financial penalty under section 6.6.6A.

These guidelines apply to both market participants and the IESO.

OVERVIEW

Steps

The magnitude of financial penalty levied on a party, will be determined in two steps:

STEP 1 - Penalty Range,

1. Impact Level
2. Non-compliance Level

STEP 2 – Fixing Penalty Amount

1. Base Amount
2. Final Penalty Amount

DESCRIPTION OF STEPS

A detailed description of the principles used in each step below is provided in the section titled “Description of Principles”.

STEP 1 - Penalty Range

There are two parts to establishing the penalty range:

1. Impact Level

The impact level is determined by examining all the impacts of the breach under investigation and selecting an appropriate impact level.

2. Non-Compliance Level

The non-compliance level is determined by assessing the level for: 1) Breach History and 2) Severity, and selecting the higher of the two, and finally, deciding whether any increasing or decreasing adjustments are appropriate. Among the adjustments that would increase the non-compliance level are: 1) Lack of Due Diligence, 2) Benefit, and 3) Corporate Intent.

For example, if the breach history is assessed as ‘moderate’ and the severity is assessed at ‘high’, the non-compliance level will be ‘high’ unless an adjustment, such as corporate intent to breach the market rule, applies. In this case, evidence of corporate intent to breach the rule would raise the non-compliance level from ‘high’ to ‘severe’.²

² Table 3 in the next section shows the non-compliance levels associated with the different assessments of Breach History and Severity.

Sanctioning Guidelines

The appropriate penalty range (bounded by the minimum and maximum amounts) is identified from the intersection of the chosen non-compliance level and the impact level of Table 1.

TABLE 1: Section 6.6.6B Penalty Matrix

Impact Level	Non-Compliance Level (Severity and Breach History)							
	Low		Moderate		High		Severe	
	Range Limit		Range Limit		Range Limit		Range Limit	
	Min	Max	Min	Max	Min	Max	Min	Max
Low Little or None	\$2,000	\$25,000	\$2,000	\$50,000	\$3,000	\$75,000	\$5,000	\$100,000
Medium Material	\$2,000	\$100,000	\$4,000	\$250,000	\$6,000	\$450,000	\$10,000	\$600,000
High Severe	\$4,000	\$250,000	\$8,000	\$500,000	\$12,000	\$750,000	\$20,000	\$1,000,000

Note: matrix can be used to assess penalties on a per breach basis or as one aggregated breach.

STEP 2 – Fixing Penalty Amount: Case Factors

MACD will establish a base amount within the penalty range selected from step 1, by examining Impact and Time Horizon of the breach. In fixing a final penalty amount, MACD will also consider additional case factors which can result in an increase or decrease from the base amount.

1. Base Amount

The outcome of Step 1, will result in the selection of a penalty range from Table 1 within which a base amount will be selected. MACD will consider the following two case factors when fixing a base amount from the relevant penalty range:

a. Impact Assessment

The impact assessment will be based on all impacts of the breach under investigation. The same criteria are applied as have been used to establish the impact level in Step 1.

b. Time Horizon

The analysis will assess the degree of immediate risk posed by the breach under investigation.

2. Final Penalty Amount

Once a base amount is determined, the final penalty amount, within the selected range in Step 1, will be determined after assessing the additional case factors. Each factor can result in an increase (aggravating) or decrease (mitigating) from the base amount.

DESCRIPTION OF PRINCIPLES

Step 1

Impact Level

The impact level determined in Step 1 will be established after consideration of:

- the impact of the breach on other market participant(s);
- the actual or potential impact of the breach on the IESO-administered markets as a whole;
- the actual or potential impact of the breach on the reliability of the integrated power system; and
- any sanctions that may be imposed on the IESO by a standards authority as a result of the breach.

Once all these impacts are considered, an impact level commensurate with the descriptions of each level in Table 2 is selected.

For breaches of reliability standards, NERC will be assigning an impact level (violation risk factors) to each requirement of a standard. MACD will take into consideration the NERC violation risk factor in determining the impact level as the assessment of the impact the breach has had on reliability. Violation risk factors for all standards have yet to be assigned. In the absence of these, MACD will make best efforts to assign a violation risk factor in accordance with the principles used by NERC or NPCC (FERC Order RR07-9-000 and RR07-1-000, issued May 18, 2007, paragraph 9). Where violation risk factors have yet to be assigned by NERC, MACD will make public the impact level used in the application of these guidelines.

Sanctioning Guidelines

TABLE 2: Impact Levels

Impact Level	Description
Low	The potential or actual impact of a breach was negligible or there was no impact.
Medium	The potential or actual impact of a breach was material.
High	The potential or actual impact of a breach was severe.

Non-Compliance Levels

The non-compliance level is determined by: a) selecting, from Table 3, the higher level determined by examining both Breach History and Severity, and b) considering any increasing or decreasing adjustments.

TABLE 3: Non-Compliance Level Criteria:

Non-Compliance Levels				
	Low	Moderate	High	Severe
Breach History	Zero or one	Two	Three	Four
Severity	Low	Moderate	High	Severe

1. Breach History

This criterion considers the compliance history of a party with breaches that are the same or related obligations to the breach under investigation. As an alternative to considering these breaches in determining the non-compliance level (Step 1), they can be considered in Step 2. MACD will not use a mechanical approach in determining the contribution to a party's breach history. Rather, MACD will have regard for all of the circumstances surrounding a party's breach history, including the significance of the breach history relative to the party's number of assets or facilities and the amount of time that has passed since the breaches occurred. MACD will also consider the extent to which a party has remedied past breaches or executed mitigation plans and the time required to do so. For example, related past breaches that have not occurred recently, that are less serious, or that were remedied quickly and effectively, are likely to be excluded from consideration.

The notional weights assigned these past breaches is described below:

- a. **Failure to Comply with Orders**
Upon a finding of breach, MACD can issue orders which can include but are not limited to any action necessary to remedy a breach of the market rules as set out in section 6.2.7. Any one failure to comply with an order will contribute to a party's breach history by a count of 'one'.
- b. **Continuing Breaches**
A breach is described as 'continuing' if a party has been found in breach of a obligation and the same breach remains unresolved. Any one continuing breach will contribute to a party's breach history by a count of 'one'.
- c. **Consecutive Breaches and Repetitive Breaches**
Each market rule obligation may explicitly state a time frame in which the obligation must be met. For example, a market rule may explicitly require that verifications be conducted annually. With breaches of this obligation that occur in 2003 and 2004, the 2004 breach would be considered 'consecutive'. If the breach under investigation is 'consecutive', the past breach will contribute by a count of 'one' to breach history.

In contrast, if breaches of the same obligation occur in 2003 and 2005, the 2005 breach is considered 'repetitive'. Two repetitive past breaches contribute by a count of 'one' to a party's breach history. In conjunction with a failure to execute mitigation plans two repetitive breaches may contribute to breach history by a count of 'two'.

Other failures may be event driven such as operating reserve activations. Consecutive breaches may occur two weeks apart or 2 hours apart depending on the timing of the activation request. Where the market rules do not explicitly state the time frame in which the requirement must be met, MACD will determine whether recurrent breaches are consecutive or repetitive.

In some reliability standards, there is a 'violation reset time' for a standard, which describes the period of time generally required for a party to continue operations without incidence of further breach of the reliability standard, in order to avoid or minimize consideration of party's previous breach history for sanctioning purposes in the event of a subsequent breach. Breaches that occur within the 'violation reset time' are likely to be considered 'consecutive' breaches. Conversely, breaches outside the 'violation reset time' are likely to be considered 'repetitive' breaches.

Sanctioning Guidelines

2. Severity of Breach

Severity will consider the number of documented instances of non-compliance (not necessarily established breaches) and the extent of the breach. Two such examples are provided below.

Example One:

Severity may be established by using a rate of non-compliance. The rate is indicative of severity and may be set at 90% or above for good performance and 75% or below for unacceptable performance. For 75% performance the non-compliance level maybe considered “severe” depending on the nature of the requirement.

Example Two:

Duration may be considered in establishing the severity of a breach. For example, the length of time a party fails to establish direct communication with the IESO after a contingency is an indicator of severity. The requirement specifies that contact be made within 5 minutes. The severity of the failure would be relative to the 5 minutes requirement and maybe considered severe if it exceeds 15 minutes. In contrast, the failure to upgrade a metering installation may be considered low if the duration of the breach is less than one month.

As illustrated in these examples, the severity of a breach must be viewed within the context of the requirement. The examples are not exhaustive of the type of assessment MACD will deploy to determine severity.

In relation to breaches of reliability standards, NERC is planning to define for each of its standards four levels that attempt to capture the severity of non-compliance, to be known as the ‘Violation Severity Level’. Where a Violation Severity Level exists, MACD will consider it as its assessment of severity to the extent it captures all dimensions of the severity of the breach.

3. Adjustments

Once an initial non-compliance level is determined it can be adjusted to a higher or lower level (adjusted to the right or left, respectively, at the same impact level). If any one or more of the following three factors are present, adjustments will be made to a higher non-compliance level (adjust to the right) along the matrix.

a. Lack of Due Diligence

This adjustment will increase the non-compliance level when the severity of a breach is increased from where it otherwise would have been where there is a reasonable expectation that action should have been taken by a party. For example, an increase will occur when detection and mitigation should have taken place sometime before the breach was discovered, either through the exercise of due diligence or other periodic actions mandated under the market rules, or through good utility practices. For example, the duration of a breach may be extended as a result of inaction by a party. When the duration of a breach is increased as a result of the lack of due diligent actions as described above, the non-compliance level can be increased above the initial selection.

b. Benefit

The non-compliance level may be increased if any benefit was obtained or may have been obtained as a result of the breach. Assessment of this factor deters parties from making economic choices to breach market rules. It also sends a clear message that parties participating in the market must establish a compliance culture within their organizations and economic choices to breach are not supported as an acceptable alternative to compliance. Adjustments will be made commensurate with the benefit gained by the party.

c. Corporate Intent

A breach will be considered deliberate if the facts of a case point to knowingly breaching a market rule. Where there is an understood corporate practice or communicated corporate intent to breach, the non-compliance level established may be increased above the initial selection.

Step 2

Fixing Penalty Amount

A base penalty amount is established within the range selected in step 1 by examining impact and time horizon. The final penalty amount will be fixed within the range selected from step 1 following consideration of the additional factors listed below. Each factor can result in an increase or decrease from the base penalty amount.

Sanctioning Guidelines

1. Base Penalty Amount

Once a range is determined in step 1, a base penalty amount is set within the range based on an assessment of impacts and time horizon described below.

The impact assessment is exactly the same as determining the 'impact level' under Step 1.

a. Impact Assessment

The contribution of 'impact' to establishing the base penalty amount is carried out after consideration of:

- impact of the breach on other market participant(s);
- the actual and potential impact of the breach on the IESO-administered markets as a whole;
- the actual and potential impact of the breach on the reliability of the integrated power system; and
- any sanctions that may be imposed on the IESO by a standards authority as a result of the breach

b. Time Horizon

The rules have requirements which span a range of time frames. Some requirements pertain to planning activities and are conducted years in advance. If these are breached, they pose a future threat to reliability or the market. Conversely, breaches affecting real-time grid operations or market outcomes pose an immediate threat. Breaches which pose an immediate threat would result in higher base penalty amounts than breaches pertaining to planning activities, all other factors remaining equal.

Reliability standards' requirements fall into similar timeframes long term planning, operations assessment, operations planning, real time operations, and same day operations. NERC and NPCC have linked these categories with the immediacy of threat breaches pose to reliability. MACD will consider these linkages in establishing a base amount for breaches which cause reliability impacts.

2. Final Penalty Amount

Additional Case Factors – Aggravating and Mitigating

The final penalty amount will be fixed within the range selected from step 1 considering the additional factors listed below. Each factor can result in an increase or decrease from the base penalty amount within the identified range:

- a. the circumstances in which the breach occurred;
- b. the severity of the breach;
- c. the extent to which the breach was inadvertent, negligent, deliberate or otherwise;
- d. the length of time the breach remained unresolved;
- e. the actions of the *market participant* on becoming aware of the breach;
- f. whether the *market participant* disclosed the matter to the *IESO* on its own or whether it was prompted to do so;
- g. any benefit that the *market participant* obtained or may have obtained as a result of the breach;
- h. any previous breach by the *market participant* of the *market rules* or of the conditions of its *licence*;
- i. the actual or potential impact of the breach on other *market participants*;
- j. the actual or potential impact of the breach on the *IESO-administered markets* as a whole;
- k. the actual or potential impact of the breach on the *reliability* of the *integrated power system*;
- l. any sanctions that may be imposed on the *IESO* by a *standards authority* as a result of the breach;
- m. the immediacy of the threat that the breach poses to the *reliability* of the *integrated power system* or the *IESO-administered market*;
- n. presence and quality of the *market participant's* compliance program;
- o. whether on its own initiative, a *market participant* has undertaken to reasonably compensate the *IESO-administered market* for the value of any benefit it obtained as a result of the breach; and
- p. such other matters as the *IESO* considers appropriate.

Examples of “other such matters as MACD considers appropriate” are past case communications concerning past remedies implemented for related breaches, the level of cooperation provided by the party in resolving the investigation will be considered, failure of a party to comply with a directive or order given by the *IESO*.

Sanctioning Guidelines

DUE PROCESS ADDITIONS

For financial penalties assessed pursuant to these guidelines, once MACD has found a breach of the market rules, MACD will provide the party under investigation an opportunity to provide additional information and comment on the preliminary penalty assessment through written submissions. Prior to issuing the final Notice of Non-compliance, MACD will issue a draft notice to the party with an attached preliminary penalty assessment.