

Proposal for changes to the EGR Compliance Regime

a view by

Transpower New Zealand Limited

System Operator

January 2007

Contents

1.	Purpose	2
2.	Background.....	2
3.	Introduction	3
4.	Regulatory Regime.....	4
4.1	Regulatory Requirements.....	4
4.2	Regulatory Process	5
4.3	Breach Statistics and Information Publication	6
4.3.1	Statistics	6
4.3.2	Data Publication, Industry Information, and Learning	9
5.	Observations and experience with compliance	9
5.1	System Operator General Observations	9
5.1.1	Breach reporting process	9
5.1.2	Settlement Process	10
5.1.3	Rule Clarity	11
5.2	Relationship between Settlement and Rule Change.....	12
5.3	Application of compliance process	14
6.	Summary of Issues with Compliance Process	15
7.	Options for Change	16
7.1	Reduction in reporting obligations and streamlined process.....	16
7.2	Settlements and Binding Interpretations	18
7.3	Transparency, Information, and Process	18
8.	The Way Forward	19

1. Purpose

This paper sets out Transpower System Operator's:

- view of what the objectives of an appropriate industry compliance regime should be
- view of perceived implementation issues with the existing compliance regime and achievement of industry objectives
- suggested changes to both processes and regulations and rules that could better achieve industry compliance objectives.

The views expressed in this paper are those of the System Operator. They arise from our own experiences with the current compliance arrangements and may not reflect the experiences of other parties and, especially, those of the Electricity Commission (EC). To that extent, our comments do not purport to represent a comprehensive, industry-wide review or commentary.

Our views are intended to be constructive and motivate efforts toward effecting change. They are not intended to express or imply criticism of any participants or the EC. To the contrary, the System Operator has since March 2004 enjoyed very good relationships with the participants and the EC in respect of compliance matters. But, we think it's time to look for improvements in the rules and how they work.

2. Background

It is helpful to consider possible changes to the compliance regime against an understanding of the broader role of and expectations around the regime.

The Government Policy Statement (GPS) makes the EC responsible for monitoring compliance, investigating alleged breaches, taking enforcement action if necessary, and establishing an independent Rulings Panel to adjudicate on alleged rule breaches.

The EC's Statement of Intent (SOI) describes its objective to be *'more than just a policeman to the industry. Instead it wishes to facilitate 'a greater understanding of and thereby improved compliance with the Rules' as well as to 'identify areas of the Rules that may need change'*. The EC has stated *'Improved compliance contributes to improved performance across the industry, and contributes to more effective rules'*; we strongly agree with this statement and think that an improved compliance process will contribute to the objective of more effective (industry) rules.

The EC's compliance performance measures (recorded in the SOI) are to:

- complete 50% of investigations for reported breaches within 3 months
- complete 85% of investigations for reported breaches within 6 months
- adhere to quality standards
- follow investigation processes
- close 180 -220 breaches (presumably within a year).

The (then) EC Chairman Roy Hemmingway¹ stated the EC's approach to compliance is to allocate resources where they are most needed and to seek evidence participants are learning when 'things go wrong'. Other stated outcomes of a compliance regime under the Electricity Governance Regulations and the Electricity Governance Rules (together, the EGRs) include the desire for process improvement and a means of identifying whether the rules are 'working'.

3. Introduction

Taking account of the regulatory background, the System Operator believes the industry compliance regime should reflect the following principles:

- be clear, so participants understand the intent of the rules and the expectations of behaviour
- be fair and able to deliver transparent, consistent, and reproducible outcomes
- be cost-effective and efficient (to ensure targets are met)
- encourage continuous improvement
- discourage repeated undesirable behaviour with appropriate incentives and sanctions
- promote effective identification of areas where the rules need to be reviewed to improve compliance and to allow the EC's advisory groups to focus on matters of strategic importance and material operational risk.

The System Operator's experience during the first two and a half years of the EGRs leads us to conclude the present compliance regime does not fully deliver these objectives. In particular:

- the process followed in respect of each reported breach:
 - is lengthy
 - in our view is not cost effective
 - fails to always deliver fairness and consistency
 - brings insufficient focus to high risk or material matters
 - does not support the SOI targets as strongly as they might
- the present implementation of compliance processes lacks sufficient transparency and could provide better confidence of consistent, fair, and reproducible outcomes
- the settlement process can be too easily derailed by a single participant, even where a majority of participants wish to settle and often results in requests for rule changes that are unlikely to be achieved in a short period of time. This results in continued lack of clarity and understanding the rules
- the compliance regime is not delivering a body of easily available precedent decisions, clarifying what the rules mean and from which participants can develop compliant processes
- the Rulings Panel has gained little experience in the industry and has played little useful or active part of the compliance regime

¹ EC Compliance Conference, Wellington, November 2005,

- the EC publishes little information about compliance performance. Participants have little opportunity to learn from the mistakes and experiences of others and are unable to measure the performance of the EC in the area of consistency and reproducibility

We believe it is now time for the existing compliance arrangements to be reviewed to aid and improve the delivery of a more effective and efficient compliance management regime. This paper explores the above observations and suggests changes to help meet the objectives noted above.

The Paper has been prepared with the objectives of:

- stimulating debate about what issues exist and what improvements can and should be made to the current compliance regime
- encouraging the industry, including the EC, to embark on a review and change process to effect rule changes that will improve the compliance regime.

4. Regulatory Regime

4.1 Regulatory Requirements

EGR regulation 62 requires participants to notify rule breaches by other participants. Regulation 63 requires participants to self report a breach of “any rule relating to quality and security in Part C and Part G”. At first glance, these provisions appear sensible. They suggest the Board (of the EC) is to only deal only with issues that have quality and security implications. The mandatory reporting by one party of breaches by another participant is probably based on the reasonable assumption that, for one participant to have noticed another participant’s breach, the breach must be serious and have had a material impact on others in the industry.

Thereby, the regulations appear to target the reporting of only serious breaches. Regrettably, the term ‘quality and security’ for the purposes of the EGRs is not defined.

Service providers are subject to an even stricter reporting regime. Regulation 45 requires a service provider to report all breaches, by itself and others, regardless of the nature and impact of those breaches. This requirement is in addition to the specific rules that require each service provider to furnish a daily report that includes any identified breaches by itself and other participants, however minor². This requirement requires reporting beyond the standard of ‘quality and security’.

The combined effect of the foregoing rules is to make all rule breaches reportable to the Board, whether minor or material.

The requirement for service providers to report all breaches by themselves and other parties appears to have been deliberately included in the EGRs. Service providers have a ‘watchdog’ role under the rules that, in general, we support. We think the inclusion was made because the Board, which is responsible for the compliance regime, needs to receive as much information as available to determine whether the rules are working. In particular, the

² Rule 9 of section III of part G

reporting of all breaches was to result in the Board (who were, at least initially, likely to be less knowledgeable about the rules than service providers), being fully informed about the industry workings and the performance of participants and the rules.

The net effect of the provisions requiring service providers to report all observed breaches (even if already reported by the participant) with there being no established 'threshold' as to what are quality and security breaches, is that, in our view, there is a substantial number of trivial non-compliances and 'possible' non-compliances reported³.

4.2 Regulatory Process

The full breach resolution process can be lengthy. Once a breach is reported to the EC, whether in a monthly or daily report from a service provider or by a participant directly, the process we have observed is generally as follows:

- EC logs the breach and assigns a reference number
- EC writes a letter to the potential breach participant requesting facts
- alleged party in breach must respond to the letter within 10 working days
- EC may request further information via a letter or a face-to-face discussion. This inquiry process may involve a number of interactions, depending on the event complexity
- EC writes a report to the EGR Committee with a recommendation to pursue or decline to pursue the breach
- EGR Committee determines the action it will take. It may decline to pursue or appoint an investigator
- if the EGR Committee declines to pursue a matter it writes to the alleged breach party and presents its view of the parties actions
- if the EGR Committee appoints an investigator, the investigator publicises the investigation and affected participants may elect to join the investigation
- the investigator writes to the alleged breach participant requesting additional facts
- the alleged breach party must respond to the letter within 10 working days
- the investigator may request further information (by letter or face-to-face discussion). Again, this inquiry process may involve a number of interactions, depending on the event complexity. All correspondence is shared with participants that joined the settlement
- the investigator attempts to effect a settlement. This is a sub-process itself and is mandated in the EGRs. Participants which join are requested to state their preferred outcomes from settlement
- participants and the investigator endeavour to agree a settlement (by meeting or by correspondence)

³ For example, timeframe breaches on the dispensation process, low impact and low duration modelling errors, two parties reporting the same breach, late delivery (by only several minutes) of daily reports, late delivery of SCADA notices etc.

- any agreement (which must be unanimous) is submitted to the Board for approval; a failure to reach a settlement is advised to the Board
- if there is no settlement, or if the Board does not approve the settlement, the Board can choose to decline to pursue the breach or to refer it to the Rulings Panel
- the Board may approve a settlement which then binds the parties to the settlement (including the Board)
- reference of a matter to the Rulings Panel (by laying a complaint) initiates an EGR-mandated process for that independent body.

4.3 Breach Statistics and Information Publication

4.3.1 Statistics

The average number of breaches reported monthly (from 1 March 2004 to August 2006) to the EC was 18 (ranging between 12 – 30). All were managed through the foregoing compliance process or relevant part thereof. The EC employs three investigators and the EGR Committee meets (on average) every six weeks. Two Board members comprise the EGR Committee.

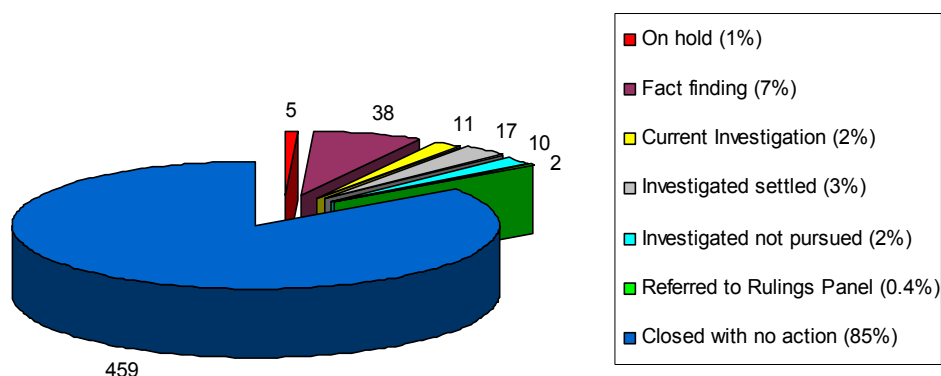
The total number of reported breaches from 1 March 2004 to August 2006, there was 542. A number of those breaches involved the same rule, though often in very different circumstances. There have been a number of repeat breaches by participants (including by the System Operator).

Our observation is that, generally, it takes quite some time to resolve many reported breaches. For System Operator self-reported breaches the average number of days from report to resolution was 114. There is evidence this is improving with time; the average drops to 75 days for breaches reported since 1 March 2005 and 52 days for breaches reported since 1 March 2006. The 52 days likely corresponds to the approximately six-week timeframe between EGR Committee meetings. However, we understand the EGR Committee is faced with a significant workload for each meeting to close out the relatively minor breaches. Notwithstanding the 'prioritisation' processes we understand the EC compliance staff use to manage breach investigations, we think that using the EGR Committee to deal with minor matters is likely to reduce the time the EGR Committee can devote to considering material matters. In our view, we think the Board should deal with matters of substance and materiality.

The following graph shows the actions taken by the EC in respect of reported breaches⁴.

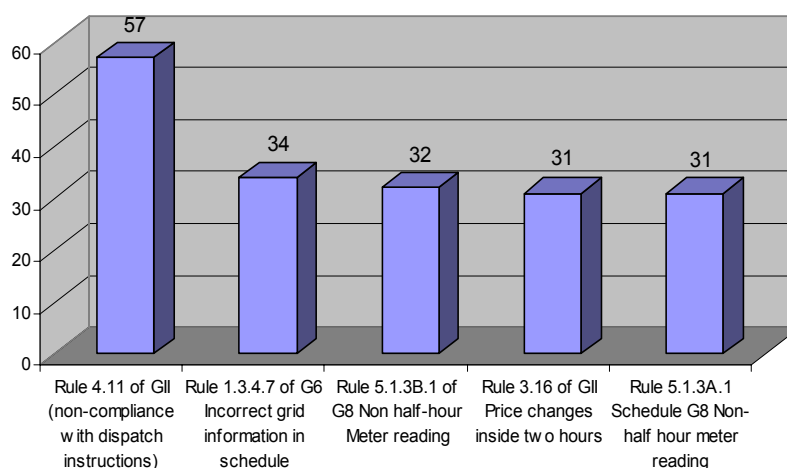
⁴ The breaches on hold relate to the non-granting of dispensations Part C. These have, in the past, been a greater number but have been steadily closed over time

Status of breaches reported from 1 March 2004 to August 2006



The following graph presents (at August 2006) the top five rules breached since 1 March 2004.

Top 5 rules breached since 1 March 2004



We make the following observations:

- consideration of the breaches of rule 5.1.3A.1 of Schedule G8 (32) were 'on hold' pending a review of the rule. The rule is poorly drafted. Notwithstanding the EC's pragmatism in treating these breach allegations as 'on hold' while the rule was under review, there did not appear to be any basis under the rules for such an approach being taken. We believe the matters have now been resolved
- the breaches of 3.16 of section II of part G were notified early in the EGR regime and COMIT was changed to make it difficult for participants to breach this rule. Few recent breaches of this rule have been reported
- the part C breaches relating to non-granting of interim dispensations were grouped together (by rule) and were effectively left to an EC Senior Investigator to follow up. These number 5 (the red section of the pie graph) but may represent more than one participant non-compliance due to the grouping methodology used. For pragmatic reasons, we understand these breach allegations were not progressed through the

investigation regime. Instead they were left until relevant rule changes were determined for part C or the Senior Investigator could work through these with individual asset owners to arrive at a solution. As noted above, it is unclear on what regulation the EC is relying to place consideration of breach allegations 'on hold'.

- the System Operator has advocated that the breaches of 4.11 of section III of Part G, be treated as a quality and security issues. The majority of these reported breaches fall into the '85% 'not pursued' portion of the graph
- the rule most breached by the System Operator is rule 1.3.4.7 of Schedule G6 (incorporation of grid owner information into dispatch), most breaches of which, in our view, have no effect on quality or security. The analysis of our breach data reveals that of the 34 breaches of this rule reported to date; only five had an actual or potential market impact. In our view, none had a security impact.

The data shows that approximately 87% of the reported breaches are not considered by the EC worthy of substantial compliance action on its part, beyond the decision to close a file or issue a letter of warning. In large measure we agree with the EC's approach, given the construction of the EGRs and the obligations on the EC arising there under. Some of these breaches are regarded as worthy of at least reprimand and special comment by the Board; we also agree with that approach. The System Operator's experience, however, is that only a small portion of the breaches reported which fall into the '87%' category are regarded by the EC as sufficiently serious to have resulted in the issue of a letter of reprimand or more.

We understand that each reported breach incident requires investigators to undertake a level (and sometimes a lot) of fact finding to determine whether a breach has or has not occurred and what view of system risk the EC compliance staff believe is appropriate to the alleged breach event. We believe it should be possible and would, in any event, be preferable to define certain breaches as minor and avoid the need every time for regulator consideration.

We also know that in respect of each breach allegation participants and the EC collectively expend a considerable amount of effort. In some cases this is appropriate; in many this is not. We think that a better division of breaches (and allegations) into important and less important at the outset would enable all involved to apply the appropriate resource to managing the arising compliance obligations.

4.3.2 Data Publication, Industry Information, and Learning

The EC has so far published little in the way of information regarding its breach determinations. Participants have little opportunity to learn from the mistakes and experiences of others. There is no publication obligation in the EGRs regarding the compliance outcomes; we think there should be.

In our view there is currently little learning available to industry from the breach management process. There is little guidance about whether the rules are actually working. There is no explicit mechanism (say, for example, a standard operating procedure) for prioritising industry and breach issues of importance. The limited guidance that is available is received, individually, by a participant when it receives a warning from the Board regarding its actions. In our experience, this is generally in a letter advising a particular matter is being taken no further by the EC.

In substance, and outside settlement arrangements, the breach management process is largely undertaken between the EC and individual participants. In contrast to New Zealand's public and precedent-based legal system, where judicial determinations are, for information and behaviour-changing reasons, reported as a matter of public policy, the industry receives little or no information from the EC about participant breach behaviour.

Some information does become available when breach matters are investigated⁵. When a settlement agreement is reached the content is published, providing further insights. However, our experience is that settlement agreements generally do not determine if there was any non-compliance and (correctly, in the context of settlements) target industry-acceptable behavioural changes. These are often operational and procedural rather than directly reflective of rule-mandated behaviour. While providing valuable insights, the settlement process provides little confidence that all reported breaches are being treated according to the same criteria.

5. Observations and experience with compliance

5.1 System Operator General Observations

5.1.1 Breach Reporting Process

Our experience since 1 March 2004 is that the compliance regime deals with all reported breaches using essentially the same initial process, regardless of operational and market impact. The majority of rules breached by the System Operator have, in our view, caused a minor or no market and operational impact. Further, they have had little or no potential to affect system security. However, reporting the breaches has resulted in large volumes of essentially unproductive (and often repetitive) correspondence with the EC, leading in most cases to a determination to take the matter no further. In some of the cases the Board, quite properly, has made observations about the System Operator's actions including calling for process and other improvements.

⁵ Only 5% of allegations have gone to investigation

We acknowledge the EC does submit certain breach cases (those it apparently views as more important) to the EGR investigation process. This effectively sorts breach notifications into more or less serious categories. However, we do not believe the sorting need only occur at the level of the EC. Participants have little knowledge from EC actions of the basis on which the EC determines which breach events are regarded as being of more or less importance and, therefore, what are regarded as matters of greater risk to the power system. There is little or no publication by the EC of the basis on which it assesses matters of risk.

We believe the standard for reporting should be set at a defined level of importance so that mandatory reporting will apply only to defined and more important breaches.

We expect the result would be less time spent on minor compliance activities (by both participants and EC compliance team members) and more time available to participants to spend on corrective actions and process improvement. If a participant has a series of 'minor' breaches and those breaches impact on, and frustrate other participants as a result, there is no barrier to participants approaching each other to resolve the issue, or reporting such breaches to the EC for resolution.

The compliance regime requires the System Operator to report all breaches it becomes aware of, by all parties and whether relating to quality and security or not. Further, even where it is aware a breach has already been reported to the EC by a participant it must report the same breach (again) to the EC. While the situation has yet to arise, the System Operator is open to being in breach because it fails to report a breach already reported to the EC by another party.

The large volumes of correspondence produced means the EGR Committee will likely only have time to review the investigator's breach summary for all reported breaches. We think the EGR Committee should spend its time only on matters of substance and value to the industry, and not be required to consider, even in an administrative way, all the minor breaches that are notified but not investigated. This would appear to be extremely cost-effective and imposes no additional obligation on participants than what they already do as part of ongoing compliance management⁶.

The System Operator also notes there is no provision in the Regulations for a party to withdraw a breach allegation once alleged. This is problematic where an allegation made proceeds to formal investigation. Such investigation then must proceed to settlement when it might more properly be immediately dismissed. This is an inefficient outcome.

5.1.2 Settlement Process

The EGR settlement process attempts to effect a settlement between all parties that join the formal investigation. A settlement must be unanimous and in practice seeks to determine non-punitive actions the alleged breach party is to take to 'settle' the admitted or alleged (but not admitted) breach.

⁶ Such reporting regime could be likened to the one that exists under the Health and Safety in Employment Act

The process has worked well when the actions are straight forward and process or other improvements are agreed by all parties. However, there are a number of issues with the settlement process:

- a formal investigation always has to proceed through the settlement process, regardless of whether the additional fact finding reveals the original decision to investigate is inappropriate. We suggest, as a minimum, the Regulations be changed to allow an allegation to be withdrawn and any investigation then underway to be abandoned
- where there is disagreement about whether a rule has been breached, a rule change proposal will often be the only acceptable outcome. This invariably means the issue is not resolved until years after the breach occurred. This situation is further explained in 5.2
- there have been a number occasions where participants have decided to simply withdraw from a settlement process part way through and after considerable time has been spent by parties attempting to conclude the process. This frustrates the achievement of any settlement given the requirement for unanimity by all original, notifying participants.
- the settlement process has a high potential for failure if participants have varying expectations of what should be agreed. Several settlement negotiations involving the System Operator as the alleged breach party have failed or have been unnecessarily prolonged when a minority (or only one) of participants to the breach have decided they won't settle, despite a majority in favour of agreement. Consequently, settlement of a particular breach can effectively be held to ransom by a single participant who, for whatever reason, does not want a settlement to occur on the basis proposed by a majority. In our view, the EGRs should permit a settlement to be effected with majority agreement, rather than a unanimous one. Given the EGRs themselves are not the result of a unanimous industry or governmental process there seems little rational basis for the EGRs to provide that settlements should be based on unanimity.

5.1.3 Rule Clarity

The System Operator is aware that a number of participants have active compliance management processes in their businesses. Most participants appear concerned about actions that may infringe the rules. However, there is little evidence of the breach management process being used to educate the industry on either what the rules mean (when this is unclear, a relatively common situation) or what standards of participant behaviour are required to ensure rule compliance.

The rule breach process makes it difficult, if not impossible in some circumstances to determine if a party is actually in breach of the rules. The settlement process and the lack of determinations by the Rulings Panel means there has been little progress in formally clarifying areas of the rules that are unclear or uncertain, especially in situations where the more material breaches or alleged breaches are concerned.

Commonly there is agreement that certain aspects of the rules are unclear.

However, discerning the correct or agreed meanings of the relevant rules is less easily achieved as for the more significant breach allegations there is substantial reliance placed on the settlement agreement process, with its uncertain outcomes. While the settlement process is a very useful one (which we believe should continue), its effectiveness has limitations when competing objectives are in play.

As noted, the rules have no guidance as to what constitutes a quality and security breach. Unhelpfully, the breach process is also not developing a body of precedent decisions clarifying what those words mean (or indeed what other rules mean).

The System Operator has been the subject of two complaints to the Rulings Panel (to our knowledge, the only references made to date). These matters were admitted breaches. The references to the Panel made it plain the Board regarded the matters as serious lapses of behaviour by the System Operator. As it transpired, in our view, the Panel did not explicitly share the view of the Board and, as well, the precedent value of the cases was diminished by the fact they were the first references to the Panel.

The absence of referrals to the Rulings Panel has at least three regrettable consequences:

1. From a compliance regime perspective the Panel meets so infrequently it has little opportunity to develop a good knowledge and appreciation of the industry and therefore the context in which it makes decisions.
2. The precedent value of its decisions is only rarely available.
3. The lack of Panel decisions gives little guidance to the Board in its handling of the breach events it must routinely deal with.

Notwithstanding our regret at the paucity of referrals to the Panel, we do not believe the Board should lower its 'referral' threshold. Full, defended hearings before the Panel are not to be taken lightly and would consume substantial resources. We believe a better approach would be to add to the panel's role by allowing it to make binding interpretations without having to do so in the context of a rule breach allegation. For example, if a participant did not agree with a particular interpretation of the rules applied by the EC, the matter could be referred to the Panel to obtain a ruling on the interpretation. This would facilitate market education and understanding, potentially provide an alternative to the settlement process or allow some settlements to be more effective and, importantly, reduce the need to effect some rule changes.

5.2 Relationship between Settlement and Rule Change

One of the stated outcomes in the EC's SOI is to identify, through the compliance regime, the areas of the rules that need to be changed.

There are several circumstances under which rule changes may be identified from the compliance regime where the:

- rules do not reflect the current accepted operational processes

- rules require clarification to make the meaning more clear. That is, the meaning is generally understood but the rules have the potential to be ambiguous, misunderstood, or applied in an incorrect context (for example, the threshold for compliance with dispatch instructions)
- meaning and intent of the rules, and hence the requirements reflected in the rules, is unclear (for example, dispatch instruction compliance for interruptible load providers)
- current requirements reflected in the rules do not meet the industry future requirements (for example, the notification of constraints).

We believe an effective and efficient process to identify, prioritise, and progress rule changes directly supports the EC objective of facilitating greater understanding of the rules and improving compliance with the rules. However, the System Operator believes the existing rule change process can be improved to better meet the stated objective. Improvements might focus on the following areas:

- rule changes identified from the settlement process could, in our view, be prioritised in a different way than currently. For example:
 - if the compliance process highlights a clear discrepancy or inconsistency in the existing rules, a case for a rule change (based on compliance) can be easily made and the rule change should be promptly expedited.
 - equally, participants (to the settlement process) may desire a rule change to improve or radically change an existing process or philosophy in the rules. In such cases, a rule change proposal may not be an effective or appropriate 'first step' to settle a breach, although it may be a desirable future industry initiative
- experience so far is that the opportunity for gaining rule clarity through the breach process is actually very limited. Yet there have been occasions where a binding determination of what a rule means in a particular situation would have been very helpful. The settlement process has generally (and understandably) meant agreements being reached without any admission of breach liability. Yet often there has remained a continuing lack of clarity about the behaviour required by the relevant rules or the relative importance of the behaviour
- where rule changes are outcomes from settlement, and where those outcomes are to result in rule clarity (but not operational changes), the lengthy rule change process means participants are continually exposed to the risk of continual rule breaches until the rule is changed
 - the current rule change process (even for 'priority' and/or apparently simple rule changes) seems to take at least 18 months. The lengthy process has resulted in a significant loss of confidence by participants in the rule change process, to the extent where participants to a settlement attempt try to avoid any need for a rule change as a settlement outcome, stating a preference to refer to the Rulings Panel or requesting a written interpretation from the EC (which is not binding). Such outcomes are unlikely to facilitate a greater understanding of the rules and will likely result in increased industry cost
- the breach process can and should be used to initiate rule change actions. Such outcomes are often desirable. The System Operator's view is the current rule change process does not provide an effective and reliable means of effecting desirable and necessary changes. We

understand this is at least partly, if not substantially the result of the parliamentary process which mandates, for example, the requirement to complete cost benefit analyses for even the most simple of administrative rule changes. There are many obstacles to improving the process, including the apparent work load and priorities of the Board.

In our view, one way of responding to the issues described above could be by ensuring there are appropriate and clear processes for interpreting the current rules and prioritising rule changes. To achieve the objectives of clarity, transparency, consistency and reproducibility, the current interpretation of the existing rules should be clear, regardless of whether a rule change is pending. To that extent:

- where the meaning of the rules is unclear, an interpretation (through the Rulings Panel) should be able to be sought before proposing changes
- rule changes made to clarify rules, rather than to change operational processes, ought to be able to be expeditiously dealt with
- other rule changes (such as those arising from settlements, industry and market changes etc) should be prioritised by agreement with the industry (with the EC to determine priority in the absence of agreement).

5.3 Application of compliance process

The Regulations specify the breach reporting requirements and outline the rights and obligations of investigators as well as the powers of the Board and the Rulings Panel. The rules do not specify any principles or processes in relation to how the compliance framework is to be implemented, such as:

- the information the Board should consider when deciding to appoint an investigator
- timeframes within which decisions about breaches must be made
- the reasons for a dismissal⁷ or reference to an investigator
- expected qualifications or attributes of inspectors
- actions to take in repeat breaches by participants
- reporting obligations of the Board to other participants.

The lack of detailed guidance in the Regulations is appropriate; the Regulations do and should provide a level of flexibility in the manner in which the Board chooses to implement the regime. However, the lack of prescription introduces the risk of a compliance process that may be less certain than desirable and that may deliver inconsistent outcomes.

The following examples demonstrate where we believe the current compliance processes could be improved to better meet SOI objectives:

- there are different compliance standards applied to different participants; the System Operator has been told directly by the EC it is held to a “higher” standard of compliance. There does not appear to be any EGR basis for applying different standards.

⁷ Whilst Regulation 67 requires the Board to inform participants of its reasons, there is limited guidance as to the detail. Therefore, the reasons may (and often are) as simple as the wording in 67(c).

- the processes applied by the EC seem to have markedly different outcomes dependent on the approach adopted by individual investigators; some investigations are characterised by a marked pragmatic objective intent on resolving underlying behaviour issues. Other investigations have a literal, rule-based compliance objective. Neither is necessarily incorrect but differing approaches may result in uncertainty for participants
- the lack of publicity of breach outcomes makes it difficult for participants to be certain they will be treated in a similar fashion to their industry colleagues. This makes it difficult to learn from the experience of others
- where participants are subject to multiple breach allegations in respect of the same rule there is no information provided to participants that provide participants with confidence there will be a consistent outcome between participants or between 'cases' for the same participants⁸
- some breach allegations have, to our knowledge, never been acted upon in accordance with the Regulations – for example, those reported in relation to initial breaches of part C and the non-granting of interim dispensations. These breach allegations appear to have been put 'on hold' until matters outside the breach process have been resolved.

Variability and inconsistency of approach are unlikely to support desirable compliance objectives of fairness, transparency, and consistency. We also believe they are unlikely to provide appropriate incentives and sanctions to discourage undesirable behaviour.

6. Summary of Issues with Compliance Process

To meet public interest and legitimate industry requirements, the System Operator believes a successful compliance regime must display effective processes and ensure resources are expended on worthy issues and cases. Doing so ensures the limited industry and regulator resources available for compliance are applied to the most virtuous cases.

The System Operator believes the existing compliance regime can be improved to better achieve desirable industry objectives. In particular, the:

- EC publishes little information about compliance performance, other participant breaches or breach outcomes and decisions. Participants have little opportunity to learn from the mistakes and experiences of others. Participants are also unable to measure the performance of the EC in the area of consistency and reproducibility
- process followed in respect of each reported breach is cumbersome and unfocused. In our view it is far from cost effective, fails to always deliver fairness and consistency, brings insufficient focus to high risk or material matters and does not support the SOI targets as strongly as they might
- present implementation of compliance processes lacks sufficient transparency and could provide better confidence of consistent, fair, and reproducible outcomes.

⁸ A number of participants have been breached many times for non-compliance with dispatch instructions in respect of various generating plant; some have been dismissed, some have been dismissed with warnings, and some have been investigated and have settled with varying results. Doubtless there are good reasons, but little, if any information is available to the industry to understand why there have been different outcomes.

- settlement process can be too easily derailed by a single participant, even where a majority of participants wish to settle
- settlement process is often used to seek rule changes to change existing process and to raise matters of industry policy as a matter of priority. This outcome may be inconsistent with an objective of delivering clarity for participants about the intent of the rules. Two issues arise:
 - in some cases rule changes are sought as part of settlement when gaining an interpretation of the existing rules would be a sufficient or better result
 - rule changes accorded priority because they arise from settlement can displace simple changes required to clarify rules. Whilst the outcome of a settlement agreement change may be desirable, the only rule changes (arising from settlement) which should qualify for priority treatment should be those required to clarify the existing rules (which should then be able to be passed quickly)
- compliance regime is not delivering a body of easily available precedent decisions clarifying what the rules mean and from which participants can develop compliant processes. A lack of such clarity is unlikely to discourage undesirable behaviour or result in continuous improvement. It has the potential to result in inefficiency, with participants repeatedly arguing rule meanings or claiming a prioritisation of unnecessary rule changes
- Rulings Panel has gained little experience in the industry and has played little useful or active part of the compliance regime. Access to and use of their independent expertise should be a key part of the compliance framework and could add a valuable contribution to advancing compliance objectives

7. Options for Change

The desired outcomes of the compliance regime are certainty, consistency, fairness, and appropriate behaviour from public and industry perspectives. We believe a number of changes can and should be made to the current compliance regime to better meet these objectives. These include changes to:

- streamline the compliance process by reducing the amount of minor (and therefore unproductive) inquiry and correspondence
- increase certainty of compliance outcomes
- improve industry knowledge of compliance outcomes.

7.1 *Reduction in reporting obligations and streamlined process*

Key issues with the current regime are the lack of discrimination between important and unimportant breach events. Without reducing the value of recording and assessing individual minor breach matters we believe the rules should:

- define what constitutes quality and security for reporting purposes, with the objective of eliminating minor infractions from the EC reporting, investigation and assessment regime. Doubtless there will be substantial debate about what defines 'minor'; however, we believe that

those breaches that fall into certain defined categories are eliminated from the current process. The categories might be defined by reference to the rules (i.e. the compliance rules would require notifications of certain defined rule breaches) and/or by the likely impact of a breach event on the system and the market judged, say, by the standard of reasonableness

- require matters not reportable to the EC to be recorded (internally) by participants and advised in a summary form to EC on a periodic basis (say, quarterly). An audit regime could allow the EC to require more information or to inspect records. The audit regime might also allow the EC to require reporting of all breaches in the event the EC reasonably believed a participant was not undertaking its compliance obligations correctly
- remove the requirement for a service provider to report a breach by a participant if it is aware the breach has been or reasonably believes will be reported to the EC by another party
- allow for participants and the EC to withdraw a breach allegation (on a specified basis)
- provide that, to the extent the EC's breach procedures are not mandated (in the rules), the EC must develop, publish and comply with such procedures (including any changes). The procedures should:
 - express clearly and simply the objectives of the compliance regime and generally how those objectives will be met
 - include a breach notification template defining the detail to be notified by the participant (about itself or, as the case requires, another participant) so that the EC or other participant can reasonably understand the general nature of the breach allegation. This would include the rule alleged to be breached and the facts alleged to constitute a breach of the rules
 - mandate the timeframes within which the Board will make its determinations
 - define the criteria on which decisions regarding the breach are to be made⁹. The criteria should be specific and contain some form of weighting as to relative importance. Such criteria, made available to participants, will then provide transparency regarding the EC's decision to dismiss, warn, investigate, or lay a formal complaint
 - outline how an investigation will be undertaken by the EC including the approach and communications protocols. The approach and protocols should require even-handedness between participants. Where, during an investigation, the investigator believes additional breaches may have occurred in relation to the events under investigation, the party involved should be given a reasonable opportunity to respond to these allegations before they are presented to the Board
 - set policy as to how rule changes will be prioritised with the intention that rule changes are prioritised according to industry benefit rather than because they arise from a settlement agreement or a particular lobby. The policy should be consistent with achieving the objectives or rule clarity and be transparent and available to the industry

⁹ This would presumably be based on the level of risk (security, market, or operational) presented by the breach

- require the EC to publish breach data and relevant analysis (see below).

In summary, the objectives of the suggested changes are to:

- reduce the number of minor breaches reported
- enhance the transparency of the compliance regime
- increase awareness of unacceptable behaviour.

7.2 Settlements and Binding Interpretations

The EGRs should permit settlement agreements to be reached by a majority rather than by unanimity. In our view this would enable industry benefits from a settlement to be gained in situations where a minority view can not be negotiated away. The retention of the Board's requirement to approve a settlement agreement would retain the power of veto to ensure the public interest is reflected and the compliance process is not otherwise subverted. Majority agreements would also reduce the costs associated with the settlement process by reducing the time and effort required to settle the breach allegation.

The EGRs should also allow participants and the EC direct access to the Rulings Panel to request binding interpretations. The Panel's costs for such proceedings should be met by the EC on the basis the industry as a whole would benefit from the rule interpretations provided.

As well as meeting industry needs the opportunity would arise for the Rulings Panel to increase its industry knowledge and thereby its ability to make consistent, good decision-making.

Access to the Rulings Panel for binding interpretations may promote better industry support for the settlement process. Where the meaning of the rules is unclear, an interpretation could be sought and the settlement process could then focus on other operational outcomes (that might include rule changes).

7.3 Transparency, Information, and Process

The EGRs should require the EC to publish data and information regarding its compliance activities. In addition to the publication requirements currently existing in the EGRs the following should be published on a routine basis:

- the participants' periodic reports of internally recorded 'non-notifiable' breaches
- summary details of all breach allegations made to or by the EC that are admitted or that are found to have been a breach by the Rulings Panel. The summary details will include:
 - the name of the participant
 - the rule(s) breached
 - the factual circumstances
 - the sanction imposed or other means by which the breach allegation was concluded, including reasons for the decision based on defined criteria
- a periodic (probably annual) analysis of industry compliance activity (breaches and outcomes) including trends in a form that reasonably enables industry compliance issues to be understood.

8. The Way Forward

The System Operator believes the issues raised in this paper are of sufficient significance to warrant wider industry discussion and development. This would be with a view to changing the Regulations and the processes relating to industry compliance and governance.

We believe a working-group, representative of the industry, should be established to further develop the ideas and the recommendations set out in this paper. That group should then promote changes in the Regulations and rules.

We understand the EC may already be developing some regulation changes and has in mind for them to be presented to the Minister in mid-2007. If so, we think it would be convenient that such changes also include the output from our suggested working group.