

II. IESO COMMENTS

A. Discretion and Business Judgment: Business Judgment, in a Generic Sense, is an Essential Element of the Proposed Standards. However, it is Appropriate to Consider Alternate Language to the Term “Reasonable Business Judgment” and to Document Cases Where Judgment Has Been Exercised.

The Staff Assessment acknowledges the need for discretion in meeting requirements of the standards but questions the proposed approach:

“... a successful security strategy cannot be implemented without flexibility and some discretion. The proposed approach to the issue reflected in the CIP Reliability Standards could allow a degree of discretion that undermines their effectiveness.”³

In particular, Commission staff question the achieving of discretion through reliance on “reasonable business judgment”.⁴ Staff’s concern is directed in part to the interpretation by the courts of the business judgment rule, specifically, that in some jurisdictions entities may be given excessive latitude by courts under this rule.

The IESO directs its comments to the reliance on business judgment, in a generic sense, leaving aside judgment on the variation in legal interpretation among jurisdictions of the specific term reasonable business judgment.

³ At p. 8, 9.

⁴ At p.9.

We suggest that business judgment in a generic sense is essential to having effective and efficient compliance with CIP standards. An example where the exercise of business judgment would be appropriate is a situation where a non-conforming cyber asset is an integral part of a larger, non-cyber system, where the cost and reliability benefit of a “quick fix”, i.e., the immediate replacement of the cyber asset, must be weighed against the cost and reliability benefit of the more comprehensive approach of replacing the larger system at a later time. The appropriate decision in such a case of capital asset modification or replacement will inevitably depend on business judgment applied to the particular circumstances.

The IESO has two suggestions that might allay Commission staff’s concerns:

- It may be appropriate to consider an alternative to the term “reasonable business judgment” that would be more generic and encompass the concept of discretion based on business-focused criteria. Such a term could be specific to ERO matters or specific standards, avoiding conflicts that might be caused by the broad applicability and legal implications of the current term.
- It may be appropriate to introduce a requirement for all instances of non-compliance by reason of business judgment to be documented and retained for audit purposes. Such documentation should include a clear description of how the entity will be non-compliant, the resulting risk to critical cyber assets, steps that are being taken to mitigate that risk, a timetable for re-consideration or remediation, and a signed statement of risk acceptance by a corporate officer. This would help ensure that entities are judicious in their application of “reasonable business judgment” and

would also provide transparency and promote industry-wide awareness of risks and vulnerabilities.

B. Level of Specificity: the Proposed Standards Embody an Appropriate Level of Specificity.

Commission staff express concern that the lack of specificity within the proposed standards "may lead to flawed implementation of security mechanisms that provides inadequate protection".⁵

The proposed cyber security standards are, in effect, performance requirements in that they require specific outcomes that, when taken together, constitute a comprehensive set of cyber security activities. Only to a limited extent do they identify the specific means of achieving those outcomes. This is therefore a specific instance of the generic of "what" versus "how" issue that has arisen frequently in the development of NERC standards.

The IESO has repeatedly argued for allowing discretion in *how* a standards requirement is met by focusing the requirement to the extent possible on the "what" needs to be accomplished (i.e., performance outcome). In effect, this approach intentionally limits specificity.

The IESO submits that the level of specificity in the proposed standards is appropriate.

The case for allowing discretion by limiting specificity is arguably stronger in the case of cyber security standards than for other NERC standards. That is because cyber security must operate in a more dynamic and uncertain environment than that of other

⁵ At p. 8.

aspects of maintaining reliability. Cyber attackers continually change their approaches and technology and use the element of surprise. Moreover, best practices and technology available to cyber defenders are also highly dynamic. For both attackers and defenders these changes have timelines ranging from a fraction of a second to perhaps hours, that is, much shorter than the months and sometimes years required to develop or modify standards.

It is in fact conceivable that a more specifically-written standard could be detrimental to reliability. For example, as implied above, a specific standard providing an effective detailed response to a threat on the day the standard is approved, could provide for and require compliance with a wrong and detrimental response the next day and thereafter. Another example would occur if a standard were drafted that unintentionally focused attention on a single class of cyber assets or processes in a manner that actually drew attention away from issues which, if properly addressed, might more effectively improve reliability of the Bulk-Power System as a whole. Cyber security of a multi-element system can be a complex matter - the optimum cyber security of a system as a whole will not necessarily be achieved by optimizing the cyber security of individual elements, given interdependencies among elements.

C. Use of the Term “Technical Feasibility”, as Provided for in CIP-005-1 and CIP-007-1, is Appropriate

Commission staff also raise concerns about references to “technical feasibility” within the requirements of the cyber security standard CIP-005-1 (R2.4, R2.6) in the

context of controls at access points to Electronic Security Perimeters⁶ and CIP-007-1 (R4)⁷ in the context of anti-virus software and malicious software prevention tools.

The term technical feasibility, in the present context, defines the physical ability of in-place equipment or software to directly conform to some requirement specified in the standards; or the ability of in-place equipment or software to perform its required function if modified in a way that would most directly conform to some requirement specified in the standards.

Technical feasibility considerations overlap with those of the exercise of business judgment discussed previously in this submission. When a lack of technical feasibility is found to apply, i.e., when a physical asset, software or business process would have to be replaced or modified to enable compliance with the standard, a business case should be initiated, analyzing the full range of options for achieving compliance. These options might well go beyond replacement or modification of a "legacy" cyber asset or process. For example, in some cases a multi-year program may already be underway to develop a "next-generation" system. Also, these systems enhancements depend on the degree to which vendors are able to improve the security of their products. Moreover, cyber assets may be only a small part of such a system. The next-generation solution might provide higher cyber security, albeit with some delay relative to the option of fixing the legacy system. The point is that the best decision in a situation where technical feasibility applies will depend on the specific circumstances.

Therefore, for the reasons given previously in consideration of the exercise of business judgment, it is appropriate to have a technical feasibility caveat in the standards.

⁶ At p. 26.

⁷ At p. 33.

Technical feasibility does not mean that responsible entities should be able to simply ignore a standard with no explanation and consequences. In those situations where technical feasibility encumbers full compliance to a requirement, we suggest that a responsible entity should be required to document the non-compliance, the resulting risk, and risk mitigation plans or strategies. We further suggest that the instance of non-compliance should be reviewed periodically, and that the documentation of non-compliance, resulting risk, and a statement of risk acceptance should be formally approved by a corporate officer.

D. Standard CIP-002-1 Should be Modified to Make Determination of Critical Assets Subject to Approval by the Reliability Coordinator.

Commission staff note the requirement for a risk-based assessment to identify Critical Assets, but state the concern that the standard “does not provide direction on the nature and scope of that methodology, its basic features or the issues it should address.”⁸

The central role of risk-based assessment in properly identifying Critical Assets is generally accepted. The IESO agrees there are grounds for concern, arising from: the large number of assessments to be performed by entities not previously subject to compliance with NERC standards and/or having limited familiarity with the Bulk-Power System,⁹ and the potential for disagreement between entities on what constitutes a Critical Asset, including the potential for entities to fail to declare assets critical in order to avoid being subject to compliance with standards.

⁸ At p. 16.

⁹ Commission staff note, at p. 13, that CIP standards will be applicable to a number of small entities. “...there is the issue of the applicability of the CIP Reliability Standards to small entities. The widespread use of Cyber Assets creates the potential for broad applicability of the CIP Reliability Standards.”

The IESO, however, does not support attempting to address the concern by modifying the standard to provide more explicit direction. An essential feature of a good assessment is the quality of the judgments that necessarily must be applied. Good assessment will always involve more than running a standard computer program, and hence, providing specific direction, while providing an illusion of greater assurance, will never be a complete solution.

The IESO suggests that much of the concern associated with Critical Asset identification could be addressed by modifying the standard to include a requirement for the entity to consult with its Reliability Coordinator, with the Reliability Coordinator to have the authority to make the final determination of Critical Assets within its territory.

The question of Reliability Coordinator approval of Critical Assets within its area can be viewed as part of the broader consideration currently being given to Reliability Coordinator's authority for approving asset designations in other aspects of reliability, for example:

- In NERC Standard PRC-023-1 — Transmission Relay Loadability, currently being balloted, the Reliability Coordinator would be required to designate those facilities between 100 kV and 200 kV that are critical to the reliability of the BES
- NPCC Criterion A3 is under discussion regarding a proposed requirement for the Area (Reliability Coordinator) to develop the list of Key Facilities.

This approach would also place ultimate responsibility with the entity having the broadest view of cyber security and overall Bulk-Power System reliability. To be clear,

the entity responsible for the Critical Asset, not the Reliability Coordinator, would continue to be responsible for meeting all applicable standards.

E. Applicability: There Should Continue to be a Single Set of CIP Standards Applicable to All Entities Having Critical Assets.

Commission staff seek comments on specific examples of different roles of entities regarding their potential impact on cyber security risk.¹⁰ It would seem Commission staff is really raising the question of whether it is appropriate that CIP standards be applicable to all entities, irrespective of their size and roles and impacts, as is the case for the proposed standards. The alternative would be to have different CIP standards for different classes or sizes of entities.

There are clear differences in roles and impacts among different types of entities. The range includes the control centers of Reliability Coordinators or Balancing Authorities. These are typically centralized and sophisticated Information Technology enterprise environments. The range also includes substations that are geographically dispersed, may be unmanned, and may have a delayed response to a system event requiring staff to be on-site.

As substantial as these role differences are, they do not justify restricting or differentiating standards requirements by entity type. NERC, in developing the CIP standards, has properly based the applicability on Critical Assets, which by definition are defined by their potential impact on reliability, surely the essential criterion for the

¹⁰ At p. 14.

applicability of a reliability standard. It follows that an entity, irrespective of its type, that is responsible for a Critical Asset, should be required to comply with CIP standards.

We note that this subject was discussed actively within the NERC standards development process, including the alternate approach of defining different classes of Critical Assets, corresponding to different degrees of criticality, where there would be one set of standards for each class of Critical Asset. The conclusion reached, in part because of the interconnectedness of cyber assets, was that adopting a single definition of Critical Assets and a corresponding single set of standards was the appropriate approach. This was ultimately accepted by all segments of the industry.

We note also that Commission staff have effectively made the case for the recommended approach of relying on a single set of standards with their reference to smaller entities:¹¹

"While the assets and operations of a smaller entity may not have a major day-to-day operational impact on the Bulk-Power System, they can provide a gateway to compromise larger entities and, when attacked simultaneously with the facilities of other small entities, in the aggregate have an adverse impact on the Bulk-Power System. Staff believes that a key to any determination of whether an entity should be covered by the CIP Reliability Standards is whether or not it is a user, owner, or operator of the Bulk-Power System that has a cyber connection to other users, owners or operators of the Bulk-Power System."

As an example, a substation could well be the connection point for several critical transmission lines. Switching for this substation might be performed remotely from another substation (i.e., not a control center). In this case, the cyber assets in both this

¹¹ At p. 13.

second substation and first substation having the supervisory control switching capability, should be determined to be Critical Assets and thereby subject to CIP standards.

F. Full Operational Testing of a Response Plan is a Best Practice that Should be Encouraged, But Not Made a Requirement at Present.

CIP-008-1 allows for, but does not require, a response plan to involve a full operational exercise; a paper drill being sufficient to meet the requirement:

RI. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following: ...

RI.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

Commission staff seek comment on whether full operational exercises should be included in this standard.¹²

It is the IESO's experience from response drills in other areas that a full operational exercise will almost invariably reveal weaknesses and learnings beyond those achievable by a paper drill. The IESO intends to assess, in consultation with stakeholders, including those having Critical Assets, whether, and if so when and how, to conduct operational testing.

¹² At p. 37.

At the same time there is no evidence that a paper drill would be materially inferior to an operational exercise. Moreover, there are clear risks that would outweigh benefits if the introduction operational exercises were not approached cautiously and systematically. Additionally, a very extensive effort will be required over the next several years to implement these standards in their present form. Taken together, these considerations lead us to the conclusion that introducing a requirement for full operational testing, by modifying the current standards and expanding the implementation workload, would not be appropriate at this time.

Respectfully submitted,

/s/ Kim Warren

Kim Warren
Manager, Regulatory Affairs
Independent Electricity System
Operator of Ontario
655 Bay Street, Suite 410
Toronto, Ontario, M5G-2K4 Canada