Introduction

As has always been the practice, LDCs are vigilant in providing security and protecting privacy and are well versed in the ever-increasing importance of information when providing good utility operations. All LDCs have taken and will continue to take appropriate actions to safeguard both information and systems from unauthorized and/or inappropriate third-party access.

Below are the detailed comments of the Electricity Distributors Association (EDA) organized as follows:

- Comments on the proposed Code amendments;
- Forward looking issues.

Comments on the Proposed Code Amendments

The EDA notes that the proposed Distribution System Code (Code) amendments do not prescribe the aspects of Cyber Security and that each LDC will be uniquely responsible for providing and managing their level and sophistication of Cyber Security. The Cyber Security Framework ("Framework") is acknowledged to be a suitable starting point to guide LDCs in documenting, testing and assessing practices and managing their evolving Cyber Security maturity. As Cyber Security standards evolve so must LDCs best practices, specifically they will need to attract and retain appropriately skilled personnel, invest in infrastructure capable of fulfilling new criteria and divest themselves of infrastructure that is no longer adequate. That rebalancing, augmenting and shedding of resources will require appropriate economic support and financial resources. All LDCs will take appropriate steps to prudently incur costs to fulfill the OEB's expectation of a favourable cost-benefit business case.

<u>Section 1.2 Definitions</u>

The EDA understands that Cyber Security concerns electronic security, therefore it is proposed that the appropriate definition of "Cyber Security" be:

> "Cyber Security" means a body of technologies, processes and practices designed to protect electronic networks, computers, software, data in electronic form, and, personal information in electronic form from attack, damage or unauthorized access.

While the Ontario Energy Board's (OEB) Framework is rooted in National Institute of Standards and Technology (NIST) standards that incorporate physical security it is not clear to LDCs that the definition of Cyber Security must extend to physical security. If the OEB considers it beneficial an appropriately worded definition of physical security should be provided. Alternatively, the OEB could translate NIST's accommodation of physical security into a revised proposed definition of Cyber Security.

The EDA also observes that the proposed definition of "Cyber Security Framework" implicitly references the documents issued by the OEB on December 20, 2017. The definition will also benefit from naming the

body that will ultimately be responsible for maintaining the Framework (e.g., in good standing relative to evolving best practices); please see the discussion provided at "Supervision and Roles".

Section 6.8 Cyber Security; 6.8.1 Reporting

The EDA recognizes that the proposed Cyber Security Self-Certification and contemplated annual Reporting and Record-keeping Requirements (RRRs) will need to be assessed for suitability for public filing. Any publicly filed materials cannot risk disclosing facts or materials (e.g., processes relied on by the individual LDC) that could compromise the LDC's provision of Cyber Security. Accordingly, the EDA proposes that the OEB's consultation with industry and other parties on the form of the annual Cyber Security RRRs explicitly address whether Cyber Security filings should be made in confidence as a routine matter.

Our LDCs members note that the inherent advantage of a scalable approach implies differing levels of Cyber Security and differing approaches to the ongoing provision of Cyber Security. LDCs and their representatives will work constructively with the OEB to ensure that the annual self-certification to be included in the RRRs appropriately align with the permissive provision of Cyber Security as set out in the proposed Code amendments and the Framework. In that consultation, LDCs may seek an ability to augment their annual self-certification with documentation of the distributor's assessment of the ongoing suitability of its current provision of Cyber Security. The EDA appreciates that the OEB is not proposing to leverage these anticipated RRR filings to make a determination of compliance, but rather that the OEB is striving to understand an LDC's Cyber Security maturity and readiness.

Section 6.8.1.1

The EDA makes no comment on the OEB specifying the frequency of reporting and raise no objection to the proposed schedule of filing the initial self-certification within 3 months of the proposed Code amendments coming into force. Our review of the proposed form of the 3 month self-certification (Attachment D to the consultation materials) did not identify any issues or any reason for filing in confidence.

Section 6.8.1.2

The EDA also makes no comment on this proposed Code amendment. Our LDC members anticipate that the certification will require documented support and the LDC's CIO, or equivalent, will be engaged in the internal processes that culminate in the CEO's self-certification.

Section 6.8.2

We acknowledge that providing and achieving Cyber Security is an ongoing aspect of the provision of distribution service. Like all other aspects of the provision of distribution service, LDCs incur costs to acquire the appropriate infrastructure and to attract and retain appropriately skilled staff. LDCs will continue to devote resource to providing Cyber Security and anticipate that the OEB will not constrain their recovery through rates.

Our LDC members anticipate that the costs they incur for Cyber Security, including the costs to evolve related business processes and practices, will be recoverable through rates. As is discussed elsewhere in this document, Cyber Security filings should be made on a confidential basis. This treatment must include applications seeking to recover costs through rates and seeking disposition of costs incurred in prior periods that were not recovered through authorized rates. The EDA notes that the OEB has previously processed rates applications that were supported by data that was filed in confidence (e.g., the recovery of Smart Meter costs). The EDA acknowledges that while this treatment does not reflect the OEB's 'business as usual' practice of requiring public filings it is necessary and essential to support the provision of effective Cyber Security. As the OEB's Notice describes, the benefits of Cyber Security are believed to exceed additional costs. LDCs are mindful of this expectation and that they are expected to provide value to the customer on an ongoing basis.

Forward Looking Issues

The EDA recognizes that Cyber Security needs and best practices will evolve. The comments below are offered so that the proposed amendments to the DSC are suitable for the long term.

Our LDC members share the OEB's concern that Cyber Security will not eliminate Cyber attacks. However, it is reasonable to expect LDCs to be prepared to repel known or run-of-the-mill Cyber events and to reduce the impact of otherwise unanticipated Cyber events. The OEB's Notice discusses the OEB's expectation that information sharing is an appropriate strategy to support LDCs as Cyber Security standards and the Framework evolve. While distributors appreciate that information sharing will create benefits (e.g., early awareness of best practices, support consistent and comparable level of protection across all distributors) they are also aware that it simultaneously risks exposing all distributors to the same vulnerabilities and precludes the benefit of diversity.

The OEB roots the need for information sharing in the observation that transmitters and distributors will be challenged to keep abreast of Cyber Security issues and risks, and, to develop strategies to maintain their individual Cyber Security capability. The EDA notes that this challenge exists primarily in limited situations where professional, managerial and executive teams lack adequate resources. The OEB's Notice does not address whether the appropriately resourced LDC can be expected to be self-sustaining with respect to the provision of Cyber Security. As the OEB's Notice references, LDCs have a long track record of information sharing. It is important to recognize that the information sharing of past periods concerned aspects of service that were commonly deployed and installed at thousands of sites and the number and diversity of installations did not yield an unmanageable security risk. Cyber infrastructure differs from conventional distribution infrastructure because it is accessible by third parties using relatively few 'paths', and that access may go undetected until the damage is done.

The EDA concurs with the OEB's suggestion that there are advantages to forming and formalizing an industry led Cyber Security Information Sharing Forum (Forum) for Ontario's electricity distribution industry. The EDA envisions that the Forum could be made responsible for administering the Framework

and for keeping the Framework current (e.g., emerging best practices, known vulnerabilities experienced in other jurisdictions or industries). Our LDC members fully expect to incur costs to responsibly contribute to the Forum's activities and operations and seek guidance on the recovery of those costs.

Applying the Evolving Framework

The EDA concurs that Cyber Security threats will become increasingly complex and sophisticated. All LDCs are motivated to constantly assess the ongoing suitability of their Cyber Security practices and strategies. While evolving the Framework will provide consistent guidance to the industry, distributors should be encouraged to adapt and evolve their provision of Cyber Security for their specific needs.

Supervision and roles

An industry led Forum that is responsible for maintaining a body of knowledge on Cyber Security and for maintaining the Framework will benefit all LDCs and should be established at the earliest opportunity. The case for the Forum becomes more compelling for those LDCs whose Cyber resources are to be continued at low levels.

Our LDC members have considered Forum leadership and governance issues. The EDA s recognizes that the Cyber Security Working Group (CSWG) may be capable of providing good leadership. LDCs also recognize that while the IESO may be capable of leading the Forum (as it has an appropriate body of knowledge, is conversant with Cyber Security risks and is taking steps to improve its provision of Cyber Security) this would transfer leadership from the distribution industry.

For purely practical reasons the EDA suggests that the OEB consider continuing the CSWG and engage it to scope an appropriate governance framework for the Forum. The EDA recommends that the OEB actively monitor this scoping for its use of best practices, when developing a suitable Terms of Reference for the Forum when scoping quorum requirements that reflect the sector's make up and that provide a good representation of the affected interests.

Resources

The EDA concurs that information sharing is likely the most cost effective way to maintain awareness of existing and emerging issues and practices, and that this option can be acted on within the shortest time. As noted elsewhere, the EDA recognizes that there are shortcomings of information sharing and seeks the OEB's explicit recognition and acceptance of them.

We reviewed the OEB's Notice carefully and inferred that the OEB understands that increased Cyber Security capabilities will only be realizable upon incurring increased costs, even under the information sharing regime contemplated by the OEB. Realistically, Cyber threats are expected to only become increasingly complex, subtle and sophisticated. The costs LDCs currently incur to provide Cyber Security should not be construed as adequate to provide appropriate ongoing levels of security.

Filings

Our LDC members acknowledge that providing good Cyber Security implies withholding details (e.g., strategies, technologies) and, accordingly, that the OEB's default policy of public filings should not apply. The EDA observes that the consequences to consumers of undue exposure or revelation are unacceptable and must be avoided.

This position should be extended to apply to both detailed materials on the provision of Cyber Security (e.g., to support self-certifications) and the portion of rate applications that seek the recovery through rates of Cyber Security costs. With respect to cost disposition or cost recovery applications, the EDA proposes filings that are processed confidentially where the resulting rates (or rate riders or rate adders) cannot be manipulated (e.g., reverse engineered) to discover any aspect of the underlying costs. The EDA further observes that processing such applications may require that the Board staff have an appropriate level of specialized technical knowledge.