Responses to Questions

Q1: Regulatory Requirements and Reporting

The EDA understands and appreciates that the OEB will want to ensure that consumers' information is being appropriately protected, and, that the information required to safely and reliably operate the electrical distribution system is secure. Our LDC members recognize that a range of reporting requirements are available to support the OEB in appropriately supervising this aspect of industry operations and that the proposed self-assessment should be performed pursuant to a testing regime, and likely other best practices.

Electricity Distributors see merit in filing updated NIST Self-Assessment Questionnaires. In future, there may be a need for greater specificity of reporting requirements in matters such as:

- Different reporting requirements may be appropriate for Information Technology (IT) versus Operational Technology (OT);
- For high risk vulnerabilities versus lower risk vulnerabilities;
- During transition periods where an LDC may, at the outset, not be able to demonstrate full compliance; and/or
- During, or subsequent to, either a mock or real cyber-attack.

It would be helpful for the OEB to articulate the purpose of any proposed reporting requirements so that LDCs can respond appropriately during both the initial scoping phase and in the future as reporting requirements are amended. In particular, it would be helpful for the OEB to document its 'need to know' and the unintended consequences that could occur in the absence of a reporting requirement. LDCs look forward to engaging with the OEB going forward on the appropriateness of, or need for, assurance by appropriately qualified third parties, further assurances, test results reports, and/or review. LDCs note that while self-assessment is a good practice it must be performed as a component of an over-arching testing regime.

The EDA believes that security will be preserved - and potentially enhanced - if filings are made in confidence. It is also noted that any public reports of cyber security preparedness will need to be aggregated or presented at a sufficiently high level so that no party can discern the specific cyber security practices or tactics deployed by a particular LDC or any gaps in cyber security.

Q2: Additional Implementation Tools and Guidance

As cyber threats are forever changing LDCs expect, and are prepared, that the provision of additional tools and guidance will be an enduring feature of the OEB's supervision of this aspect of the industry. LDCs look forward to learning about the steps the OEB will take on an ongoing basis to ensure that cyber security tools and guidance are capable of fulfilling consumers' expectations and of supporting LDCs in providing

service on a continual basis. Accordingly, LDCs seek information from the OEB about the transition processes between an existing set of tools and its replacement.

Q3: Adequacy of Guidance on Integration with Privacy Requirements

LDCs have appropriately integrated privacy requirements into their day to day operations, for example to comply with the Affiliate Relationships Code. Some LDCs expressed that the OEB consider endorsing the principle that OT should have ongoing access to the customer information necessary to support their operation according to design parameters. The issue of the appropriate protections (e.g., through contractual terms) governing third parties' access to information when, for example, providing IT or cyber security services or directly connecting to the LDCs information systems needs to be addressed in clear terms.

Q4: Other

The EDA would appreciate insight into whether the OEB contemplates making cyber security a subject of benchmarking. While distributors look forward to the benefits that benchmarking can reveal, they also recognize that reported results will require confidentiality, anonymity or aggregation to avoid revealing vulnerabilities or successful strategies.

An unaddressed question concerns mergers and amalgamations. The EDA proposes that, among other things, the OEB give due attention to the cyber security specific expectations that such a transaction will be expected to satisfy, to the timeline under which a transition to a single standard will be expected (or if it is acceptable for different standards to persist over the long term).

EDA LDC members are concerned that they will incur incremental capital (e.g., servers) and incremental operating costs (e.g., consultants, contractors, subscription fees) when fulfilling the OEB's expectations of cyber security as well as when complying with reporting requirements. Electricity Distributors assume that the costs of all cyber security related activities will be dealt with through rate rebasing applications and that non-rebasing LDCs will be eligible to record the incurred costs in a deferral account. The EDA notes that there is little information as to how, for example, prudence or cost effectiveness would be addressed and recognize that spending related to cyber security requires confidentiality. The OEB Staff Report identifies a Centralized Compliance Authority without explaining either its role or purpose and, of special concern, how it will be funded or resourced. The staff report sets out that participation in the Cyber Security Information Sharing Forum will be mandatory without scoping the extent, nature, purpose or resources (e.g., staff, financial) of participation. The EDA considers it desirable for the OEB to authorize a universal deferral account for all distributors to use that will record the costs incurred to achieve compliance with all the different cyber security initiatives.

In addition to the rate making treatment of the costs that will be incurred there is a question of the duration of the period available to achieve compliance with the OEB's cyber security framework. LDCs always work on a best efforts basis to achieve compliance within the specified timeline. Depending on the availability of appropriately skilled staff or consultants, and the co-ordination required to adhere to the timelines of other IT projects some LDCs may require longer periods to deploy the OEB's cyber security tools and to fulfill expectations. It would be useful for the OEB to allow flexibility.

The EDA recognizes that it will be important for the OEB to give due attention to the risks that must be managed as cyber security systems are designed and administered by humans. It is well recognized that today's most common vulnerability is people and that social engineering can give rise to significant breaches in cyber security. This attack surface requires careful attention, in particular, from the governance perspective.