Ontario Energy Board

Staff Report to the Board

On a Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors

EB-2016-0032

June 1, 2017

This Page Kept Intentionally Blank

Executive Summary

On February 11, 2016, the Ontario Energy Board (OEB) issued a letter announcing the *"Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario"* [Cyber Security] initiative.[1] The objective of the initiative described in the letter was to review the state of cyber security of the (non-bulk) electrical grid and associated business systems that could impact the protection of personal information and grid reliability.

The OEB has initiated the consultation to develop a policy and reporting requirements that provide a measurable assurance from Ontario's regulated natural gas and electricity companies that they are taking appropriate action with respect to their security, reliability and privacy obligations. To do this OEB staff is recommending the industry implement the framework by the regulated companies to provide the necessary measures of compliance and assurance that the entire network of Ontario distributors is addressing cyber security in a consistent manner and to ensure it achieves the OEB's expectations for reliability, security and privacy.

In the absence of a recognised sector specific standard or framework, the OEB has undertaken this initiative to facilitate the development of the framework so that the sector entities are able to address cyber security risks based on a consistent approach and criteria, in order to meet their obligations. Although the main the focus of the policy consultation to date has been on electricity distribution, OEB staff is of the opinion that the proposed framework and reporting requirements may also apply to non-bulk transmission[2] and gas distribution.

This *OEB Staff Report to the Board* (Staff Report) provides context and information regarding the proposed Ontario Non-Bulk Energy Sector Cyber Security framework. It describes the proposed regulatory expectations and provides a general description of the process and tools outlined in the companion White Paper, *"Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets."*

[1] 2016 – OEB - Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario (EB-2016-0032)

[2] Non-bulk power system refers to facilities and assets used in the local distribution of electric energy. A bulk power system (BPS) is a large interconnected electrical system made up of generation and transmission facilities and their control systems. A BPS does not include facilities used in the local distribution of electric energy. Bulk power systems are overseen by the North American Electric Reliability Corporation (NERC). In Ontario, the IESO determines the listing of facilitates, elements associated with bulk-electrical system (BES).

Cyber Security Landscape

The business landscape of the energy sector is continually evolving with a growing reliance on new technology and automation to perform business transactions and system operations, along with the increased use of third-party service providers and the increasing number of other entities that interface with the systems. This evolution results in greater exposure to cyber-attack. Unlike many other sectors, the geographic span of distributor assets to serve customers only adds to the exposure.

Cyber-attacks are increasing in number and sophistication globally. Adversaries collaborate and share techniques and viruses, while state-sponsored cyber-attacks can be particularly devastating. Cyber-attacks take many approaches, from targeted attacks to random phishing that may attack any utility, no matter the size.

Cyber-attacks and other risk factors include attacks through staff who may unwittingly open up a malicious virus in an email; third party service providers who connect to distributor systems to provide billing, meter reading and other services; unpatched vulnerabilities or supplier automated patching, to name a few.

Current Standards and Requirements

Cyber security and privacy are inextricably linked in Ontario. Cyber security is about protecting and controlling information and the operating systems supplying energy to consumers. Privacy is about recognising that the collection, use and disclosure of personal information are a matter of energy consumers' individual consent and personal preferences.

The OEB has set out expectations for electricity distributors and transmitters regarding both cyber security and privacy through its Renewed Regulatory Framework. These expectations, as identified by OEB staff include the need to protect the confidentiality of consumer information, protection of network systems and operations from risks related to cyber-attacks, that distributors are to ensure their system plans include appropriate consideration of these risks based on industry best practices. Further the OEB has expressed the view that it expects the industry to adopt standards and ensure it is meeting best practices.

Transmitters and Distributors already have obligations to manage cyber security and privacy risk through licence conditions and various code requirements. Under the renewed regulatory framework for electricity distributors, licenced entities must

incorporate security risk mitigation (including privacy and cyber security risks) as part of their existing filing requirements[3] supported by their Distribution System Plan.[4]

Unlike the bulk electrical system (BES), where NERC[5] Critical Infrastructure Protection (CIP) standards apply, non-bulk transmission and distribution systems do not have a standard or framework focussed on cyber security and privacy risks for the sector. Many general methodologies exist for critical infrastructure operators to select, interpret and apply.

Distributors currently develop their cyber security postures based on their own risk assessment. Distributors determine which methodology is the best fit, and then interpret that methodology in order to apply and implement the necessary controls. A lack of consistent criteria leaves each sector operator to apply its best judgement without the benefit of comparability and collaboration. These results in a challenge to the OEB in achieving its mandate to: assure the protection of assets, operations and business systems as well as consumer privacy.

Policy Initiative – Process and Consultation

This policy initiative has been guided by the engagement of many sector stakeholders: (electricity distributors, electricity transmitter, Independent Electricity System Operator (IESO) and a natural gas distributor). The Cyber Security Steering Committee (CSSC) comprised of the Electricity Distributors Association (EDA), distributors' senior leadership, IESO, academics and a gas distributor provided strategic direction for the development of the framework. A large Cyber Security Working Group (CSWG) consisting of a significant number of distributors in the province, the Ministry of Energy, the EDA, a natural gas distributor and the IESO were actively engaged in the process to evolve the framework as it is presented. The OEB also engaged an industry expert consulting team led by Acumen Engineered Solutions International (AESI) and augmented by DLA Piper (Canada) LLP and Richter LLP. This team brought experience and knowledge of the cyber security issues in the North American distribution sector, and in particular, in Ontario.

AESI was commissioned to prepare the proposed framework, with the advice and guidance of the CSWG, by creating the process and tools to manage cyber security in a manner consistent with the mandate set out by the OEB. The associated White Paper describing the proposed framework has been developed through an iterative

[3] 2013 – OEB Distribution Systems Plan p.5 and RRFE Report: p.35
[4] 2013 – OEB Distribution Systems Plan p.5, p.20 – 21 "Cyber—Security, Privacy "Where applicable, provide information showing that the investment conforms to all applicable laws, standards and best utility practices pertaining to customer privacy, cyber-security and grid protection, and p.25 "description of how advanced technology has been incorporated into the project (if applicable) and including how standards relating to interoperability and cyber security have been met.
[5] NERC – North East Reliability Council

process with the CSWG. The proposed framework is consistent with the strategic direction of the CSSC and incorporates practical tools and mechanisms to support the understanding and implementation of the framework as identified by the CSWG.

Proposed Ontario Cyber Security Framework

The OEB will be assured of cyber security compliance, supported by reporting against this common framework. The structure of the framework leverages critical infrastructure and privacy protection approaches[6] and provides sector specific context. The proposed framework has been developed by the industry as a guide to managing their cyber security and privacy risks. It provides a methodology and tool set to assess inherent risk, define the benchmark objectives and measure progress toward those objectives. This approach will ensure a consistent methodology in identifying gaps and assessing results within the sector and will support peer collaboration. By the industry establishing and applying the proposed framework, along with reporting mechanisms, the OEB will be assured that the industry is meeting its responsibilities.

The proposed framework relies on a set of distribution-focussed questions which guide a distributor to assess and determine their inherent risk level, and lead them to a recommended set of cyber security objectives that would be appropriate for that level of risk. Distributor self-assessments would be used to identify their actual cyber maturity level and any security gaps. The results would form the basis for a distributor's plans to address cyber security and privacy threats (including those that result from interactions with their service providers[7] and interconnected customers[8]) and certify its cyber protection readiness.

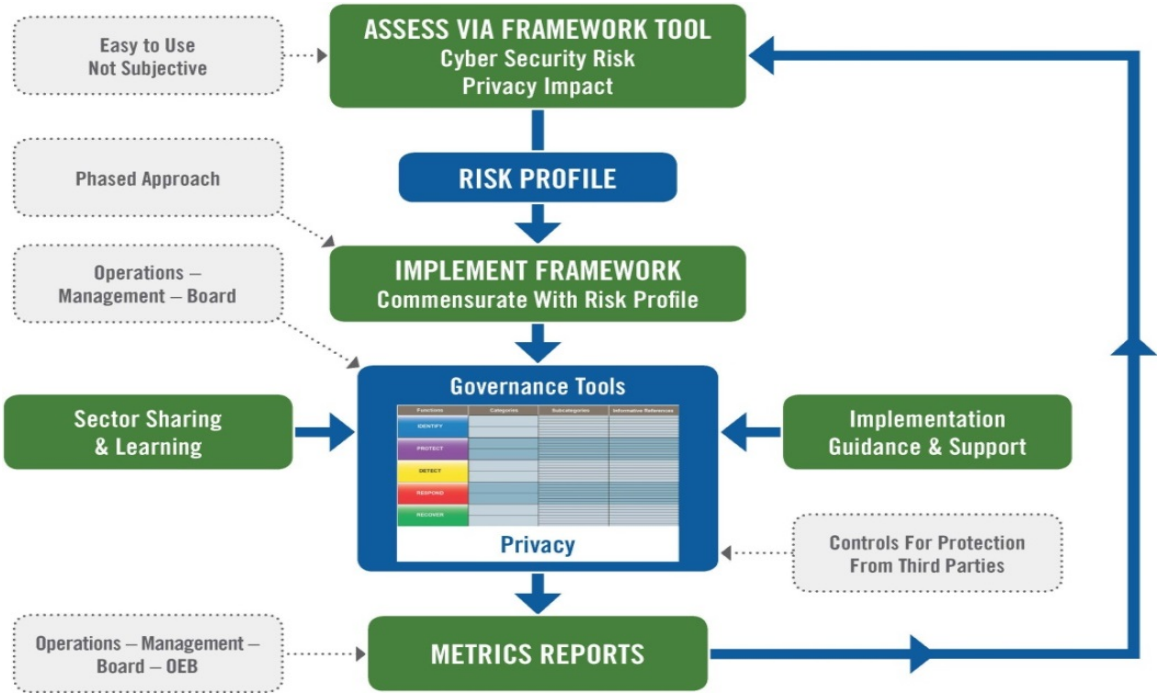
The benefits of the proposed framework are:

- It leverages authoritative approaches (NIST and ES-C2M2)[9] that are being used by an increasing number of critical infrastructure operators;
- It integrates privacy principles (PbD)[10];
- It incorporates sector-specific attributes that focus the application of NIST to the distribution sector through a set of tools and mechanisms;
- It is scalable so that cyber maturity aligns with risk;

[6] NIST - National Institute of Standards and Technology; ES-C2M2 – Electricity Subsector Risk Management Process and the Cybersecurity Capability Maturity Model; and Privacy by Design - PbD
[7] Service Providers refers to third parties entities that provide services to the distributor supporting their ongoing operations
[8] Interconnected Customers refers to companies that interact with the distribution system, such as generators and load customers
[9] NIST - National Institute of Standards and Technology; ES-C2M2 – Electricity Subsector Risk Management Process and the Cybersecurity Capability Maturity Model
[10] PbD – Privacy by Design

- It proposes a set of benchmark control objectives for different risk levels; and
- It provides distributors with flexibility in how they achieve their cyber security objectives.

The following figure provides an illustrative overview of the proposed Framework methodology.



Implementation

Phase 1 of the consultation focused on distributors requirements. The Framework is expected to be in place in late 2017 and OEB staff is recommending interim reporting by LDCs on cyber security assessment and progress provided within three months of the framework being issued, and an annual certification of cyber security capability starting in 2018. Self-certification will provide the OEB with confirmation that a distributor has assessed its risk, established cyber security objectives and assessed its current capability in meeting those objectives.

Evolution of the Framework

As cyber security and privacy risks continue to grow, distributors will be challenged to keep abreast of the evolving landscape. The OEB expects that the sector will develop a cohesive approach to addressing these risks through cyber intelligence sharing and ongoing solution development.

In proposed future phases, the OEB will facilitate the continuous improvement of the Framework through ongoing sector consultation with a broad spectrum of third party

stakeholders and regulated entities. This collaborative approach will support the OEB's expectation, that the industry developed Framework continues to evolve and improve through shared sector ownership, maturation and increased industry collaboration.

To encourage sector collaboration, OEB staff's proposals include a requirement for mandatory participation in a *"Cyber Security Information Sharing Forum"* (CSIF) where the industry comes together to promote sector collaboration, awareness and training.

Staff is suggesting the sector establish an industry-led advisory committee that would assume the ongoing management and evolution of the framework and the CSIF, similar to Regional Planning for Electricity Infrastructure[11] and the Electronic Business Transaction (EBT)[12] standards.

[11] 2011 - OEB - Regional Planning for Electricity Infrastructure (EB-2011-0043)
[12] 2003 - OEB - Electronic Business Transaction (EBT) Standards (RP-1999-0032)

Table of Contents

This Page Kept Intentionally Blank

Introduction

On February 11, 2016, the Ontario Energy Board (OEB) issued a letter announcing the *"Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario"* [Cyber Security[13]] initiative. The objective of the initiative as described in the letter was to review the state of cyber security of the (non-bulk) electrical grid and associated business systems that could impact the protection of personal information and grid reliability. The focus was to:

- Provide advice to inform the development of the OEB's cyber security policy and reporting requirements;
- Leverage best practices currently implemented by licensees;
- Ensure alignment with emergent industry standards; and
- Establish a sector-wide coherent framework for assessing and managing cyber security risks.

OEB staff worked with representatives from the industry to develop a proposed cyber security framework that addresses the OEB's expectations by providing a consistent foundation for distributors to:

- Assess their risk;
- Reference the critical controls for their risk level;
- Assess their posture against the controls and take the appropriate steps to address any gaps identified during the assessment;
- Implement governance to manage cyber security; and
- Provide the OEB with assurances that they are achieving the appropriate level of cyber maturity.

This *OEB Staff Report to the Board* (Staff Report) identifies the issues related to cyber security and privacy that OEB staff suggest should be addressed by the regulated sectors and proposes an approach for the OEB to achieve its stated

[13] 2017 - ITU—T.1205; Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organization and the users' assets. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

expectations with respect to cyber security and privacy. OEB staff's proposed approach relies on the adoption by the industry of a framework for evaluation and assessment of cyber security risks. The Staff Report describes the proposed framework and regulatory requirements that OEB staff believe will be necessary so that the OEB is provided assurances that Ontario distributors are addressing cyber security in a consistent manner and to ensure that the OEB's expectations for reliability, security and privacy are met.

The proposed framework incorporates feedback from the Cyber Security Steering Committee ("CSSC") and the Cyber Security Working Group ("CSWG")[14] as well as insight from industry experts familiar with North American distribution systems, cyber security, privacy and governance.

The White Paper, "Cyber Security Framework to Protect Access to Electronic Operating Devices and Business Information Systems within Ontario's Non-Bulk Power Assets" describes the proposed framework in detail. The White Paper is based on industry input and advice. OEB staff has approached this policy initiative in the role of facilitator, with the mandate of incubating the development of the initial framework and setting the foundation for the long-term, sustainable objective of having the sector assume overall accountability for the management of the evolution of the framework

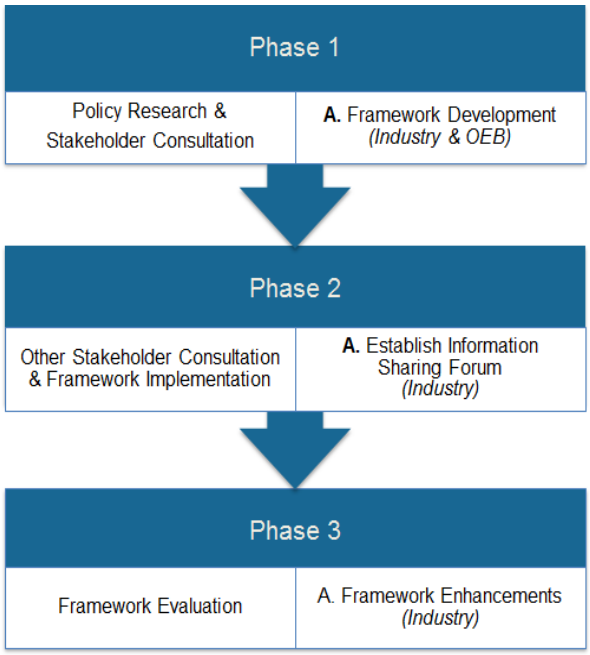
The Staff Report is organised into several sections: policy development process and consultation, background and regulatory overview, existing environment and sector research, framework foundational elements, a high-level overview of the proposed framework, measures and controls, the measurement criteria for assessing effectiveness and a proposal for implementation.

[14] Reference Appendix A, for listing of Cyber Security Working Group and Steering Committee participants

Developing a Proposed Cyber Security Policy Approach

The OEB has recognised the need to address cyber security in the electricity sector through a phased approach that reflects the complexity and evolutionary nature of cyber readiness and the breadth of stakeholders that potentially impact privacy and grid operations.

Electricity transmitters and distributors, as well as natural gas distributors in Ontario, already have regulatory obligations to manage cyber security and privacy risks. In the absence of a recognised sector specific standard or framework, the OEB has undertaken this initiative to facilitate the development of a framework so that the regulated companies are able to address cyber security risks based on a consistent approach and criteria, which in turn will provide the OEB with the assurance that the companies are meeting their obligations. Although the main focus of the consultation has been on electricity distribution, OEB staff suggests the proposed framework and reporting requirements would also be appropriate to apply to non-bulk transmission and to natural gas distribution.



This first phase has been facilitated by OEB staff, working with the industry to address the distributor business (privacy of information) and the protection of the core distribution and non-bulk transmission systems through development of a proposed cyber security framework for Ontario. The implementation of the framework is expected to be carried out in several phases over a multi-year period. The goal is to have an industry developed and implemented framework in use by the electricity distributors across Ontario by fall 2017.

In the next phase, OEB staff is proposing to work with the industry to establish a *Cyber Security Information Sharing Forum (CSIF)* to increase sector information sharing. OEB staff is also recommending the ongoing evolution of the framework be

undertaken by an industry led *Cyber Security Advisory Committee (CSAC).* The operation of the CSAC should, in OEB staff's view, be similar to that of the OEB EBT Advisory Committee[15] and the Regional Planning Advisory Working Group.[16] Evaluation of the efficacy of the framework and its evolution to meet distributor requirements and address the evolving nature of cyber security can be addressed through the CSAC.

To support the ongoing efficient evolution of the framework, it has been suggested that the Ontario sector engages with the larger US distributor associations and participate in sharing knowledge, implementation and operational methodologies. Further discussion within the sector would also be required to develop the appropriate security mechanisms for electricity and natural gas distribution in Ontario.

A follow-on phase is expected to be initiated in summer of 2017 to engage with unit sub-meter providers, retailers and marketers that provide services directly to consumers and may impact consumers' privacy and operation of the grid. As part of this phase, the OEB expects to extend regulatory reporting and the application of this framework to provide additional oversight and validation of measures taken by these regulated entities.

As part of the OEB's collaborative approach, OEB staff recommends discussions with other regulators in order to promote the broader acceptance of a common cyber security framework.

This policy consultation was designed to engage with industry to elevate the level of understanding and commitment to the sector as well as leverage distributors' existing best practices. To develop the proposed framework, OEB staff created a unique model with senior leaders from the industry and a broad-based working group that was supported by expert consultants. Extensive and ongoing sector outreach was employed throughout the consultation in order to update sector stakeholders. These consultations were instrumental in the development of the proposed framework.

Cyber Security Steering Committee (CSSC)

The CSSC was comprised of executives from the electricity and gas distribution sectors, IESO, the EDA, legal and academia. This committee met several times, initially to establish guiding principles and later to provide further direction to the

[15] 2003 – Electronic Business Transaction (EBT) Standards (RP-1999-0032)
[16] 2011 - OEB - Regional Planning for Electricity Infrastructure (EB-2011-0043)

CSWG. The five principles noted below were established by the CSSC to guide the framework's development.

- *Flexible and Sustainable: The framework will be flexible such that it will have the ability to accommodate the constantly evolving technologies of the cyber security environment and allow regulated entities to implement obligations in a manner appropriate to their relative risk profiles.*
- *Measurable: The framework will have clear measures to communicate its implementation success across the sector and further provide data to the OEB to enable audit and compliance activities.*
- *Efficient and Aligned (Standards & Privacy): The framework will achieve efficiency by considering the dual factors of cost and time effectiveness in implementation. It will further ensure that any embedded regulations, standards, and/or guidelines are robustly aligned with internationally recognised standards for cyber security.*
- *Continuous Improvement: The framework will encourage cooperation, collaboration and learning among regulated entities to support continuous improvement.*
- *Innovation: The framework will encourage and support innovation within and among regulated entities. The adoption of innovation will be supported by all of the framework's Guiding Principles and be further guided by each individual entity's self-assessment of reasonable risk.*

To provide further guidance on framework development, the CSSC recommended to:

- Use the NIST framework as the logical starting point for establishing a Cyber Security regulatory framework;
- Update the cyber security requirements within the distributors' licence and transmission system/distribution system; and
- Contain and isolate cyber security intrusions so that distributors will not impact each other through connectivity.

Cyber Security Working Group (CSWG)

The CSWG was tasked with developing the framework through a series of workshops. The first of several workshops was held in June 2016 and a significant number of the electrical distributors and one major natural gas distributor, as well as the IESO, EDA and other interested parties, were engaged. As this consultation progressed, additional distributors joined the CSWG. The workshops focussed on:

- Testing appropriateness of potential reference frameworks, leading to agreement to apply NIST, C2M2 & PbD as foundational authoritative frameworks;

- Reviewing environmental scans of the sector developed by the consultant;
- Controlled Group calibration of the proposed framework[17], Risk Profile[18]and SAQ[19] tools in order to refine the tools and set criteria and weightings;
- Review of proposed accountabilities, practices, and audit and self-assessment approaches, including third party audits and reporting models; and
- Discussions related to security cost implications.

The proposed framework is the result of the input and advice from the CSWG, specifically recommendations that the framework:

- Leverage a leading framework that is already being used by critical infrastructure sectors;
- Apply distribution business criteria to the framework to make it directly applicable to the sector;
- Minimise rework for distributors that have advanced cyber security maturity;
- Establish objective measures to support 'self-assessment' and auditing;
- Set outcome-based cyber security objectives that are not prescriptive;
- Make it scalable so that risk defines the benchmark outcomes; and
- Require assurance of compliance with cyber security objectives without operational details.

Industry Experts

The OEB engaged AESI – along with DLA Piper and Richter (the Industry Experts) who brought experience and knowledge of the cyber security issues in the North American distribution sector and in particular, in Ontario. AESI is a leading firm working with North American distributors. DLA Piper provides advice on cyber security and privacy compliance, with specific Ontario knowledge and experience in working with electricity distributors. Richter advises on in risk management and auditing across multiple sectors. Working with the CSWG, the Industry Experts were tasked with creating the White Paper that included the proposed framework.

Sector Surveys

An initial survey of the CSWG members, followed by three surveys of the other electricity and natural gas distributors assessed the cyber threat landscape, cyber security accountability allocation and current sector audit practices. One-on-one

[17] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework
[18] 2017 - Framework Risk Profile Tool
[19] 2017 - NIST Privacy Security Controls Self-Assessment Questionnaire (SAQ)

interviews with several distributors were conducted to assess their existing cyber posture in more detail.

These surveys were used to further define cyber sector issues, including identifying areas for potential risk growth and alternative courses of action. The survey results lead the CSWG to conclusions that:

- Many distributors have cyber security strategies in place and already include audits to assess their cyber posture effectiveness;
- The distributors leverage a mixture of different standards, frameworks and best practices which are not always comparable from utility to utility;
- Distributors are looking for common criteria in order to assure themselves that they are taking the appropriate actions;
- Smaller distributors do not have the capacity to apply a framework without support; and
- Distributors expressed concern about the level of effort and cost to address this risk.

Background

On October 18, 2012, the OEB issued its *Report of the Board on a Renewed Regulatory Framework for Electricity; A Performance-Based Approach*[1], which lays out the direction for the new framework and included implementation and transition plans. The OEB also expressed the view that the renewed regulatory approach recognises the need for significant investment in the sector while acknowledging that concerns over bill increases are leading to a sharper focus on the total cost of electricity to consumers. The OEB expressed that under an integrated approach, all categories of network investments will be planned together, including smart grid development and implementation.[20]

The OEB issued its *"Supplemental Report on Smart Grid"*[21] on February 11, 2013. The Report provided the OEB's response to a Directive issued by the Minister of Energy[22] requiring the OEB to provide guidance to electricity distributors and transmitters regarding its expectations with respect to the implementation of a smart grid in Ontario. The Directive set out a series of principles that the OEB should consider in setting out its guidance, one of which dealt with cyber security:

> *"…Cyber security and physical security should be provided to protect data, access points, and the overall electricity grid from unauthorised access and malicious attacks…"*

In the Supplemental Grid Report, the OEB established its expectations for electricity distributors and transmitters, including that they should take into consideration cyber security and privacy as they plan for the modernization of their systems. The OEB also concluded that

> *"…The Board will not develop its own set of cyber security and privacy standards, but instead, will require regulated utilities to provide evidence of meeting appropriate cyber-security and privacy standards.…"*
>
> *"…The Board believes that the area of cyber security is particularly suitable for future discussion and advice from the Working Group. The development of standards and practice in this very complex field will require the continued monitoring of developments in other jurisdictions to ensure that regulated entities are following best practices…"* [23]

---

[1] 2010 – OEB - RRFE Report, *Renewed Regulatory Framework for Electricity Distributors: A Performance-Based Approach* (EB-2010-0377, EB-2010-0378, EB-2010-0379)
[20] 2013 – OEB – Policy Guidance on Smart Grid Development: Renewed Regulatory Framework for Electricity (EB-2010-0377)
[21] 2013 – OEB - Report of the Board Supplemental Report on Smart Grid (EB-2011-0004)
[22] 2010 – Directive issued to the OEB – Minister of Energy – Order in Council
[23] 2013 – OEB - Report of the Board – Supplemental Report on Smart Grid, p 19

In 2015, the OEB`s Smart Grid Advisory Committee[24] was asked to assess the current state of cyber security for distributors. The committee surveyed electricity distributors and concluded that there was a wide range of understanding and cyber readiness in the sector. Most of the respondents confirmed that executive accountability was in place, however, few had a fully developed response and recovery plan. Information sharing amongst the sector was limited. A key finding was that smaller distributors were less developed in their cyber security understanding and preparedness, while the larger distributors were investing heavily in their cyber readiness.

Based on the OEB's policy statements, OEB staff suggest that the key expectations for a cyber security framework are to ensure the privacy of consumer information and that the electricity networks are reliable and maintained in a secure manner to address cyber risks.

Further, OEB staff also understands that the OEB does not intend to establish standards, but expects the industry to ensure it is meeting these responsibilities and adopting industry best practices to do so. The OEB requires sufficient and reliable reporting upon which to assess whether these expectations are being met, and therefore in OEB staff's view, the framework must support reliable and credible reporting.

Bulk Transmission System Cyber Security

Bulk system assets must comply with continent-wide cyber security standards. The North American Reliability Corporation's (NERC), the standard setting body for the bulk electricity system (BES), has developed the NERC Critical Infrastructure Protections (CIP) standards for the BES. These standards are focussed on the protection of critical assets, including the critical cyber assets. The IESO, as Ontario's reliability coordinator, has a core responsibility to ensure that the Ontario bulk electricity system is compliant with these standards and is secured against threats, including those related to cyber security. Standards are applied by bulk system operators (i.e. Hydro One Networks Inc.) and monitored for CIP compliance.

[24] 2011 – OEB - Smart Grid Advisory Committee

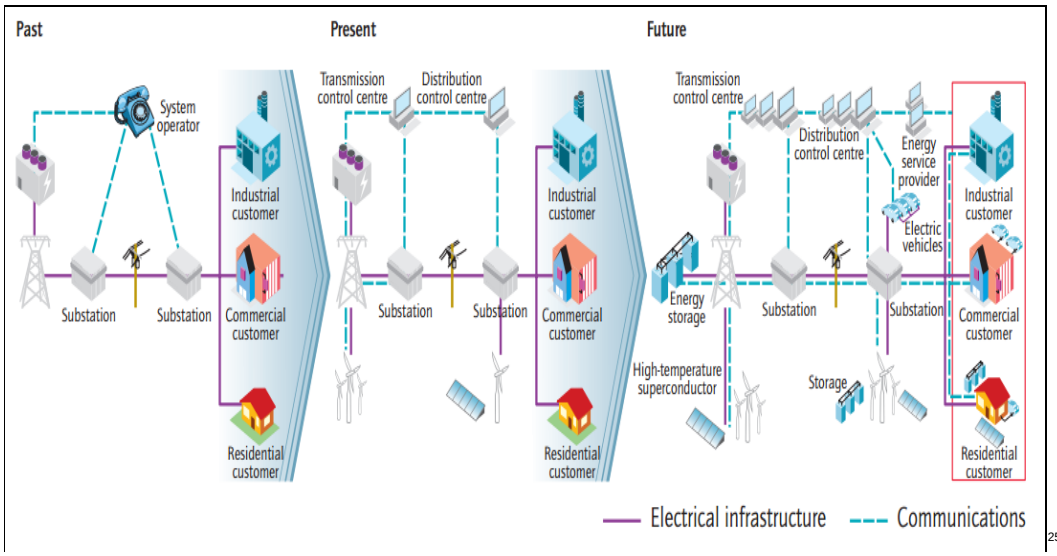
Non-Bulk Transmission and Distribution Cyber Security

Local distribution systems and electricity transmitters with non-bulk assets are not covered by the NERC CIP standards. Currently, standards or frameworks specifically developed for the distribution sector do not exist. Distributors and non-bulk transmitters have sought out, interpreted and applied various generic frameworks to achieve their own measures of privacy and system integrity objectives.

Cyber Exposure Increasing

The use of automation to enhance operational efficiency in the distribution business and the grid is evolving.

Smart grid enhancements, interoperability, the advent of self-sustaining microgrids, as well as distributed generation and demand response plans increase interdependence and interactions between entities attached to the grid. Each connection has the potential to affect the reliability of the grid. This evolution has resulted in increased risks to the reliability of the energy system due to security breaches and increased exposure to cyber-attacks and cyber-crime.



[25]

[25] 2011 - IEA; Smart Grids Roadmap

Cyber Attack Risks

Energy sector participants and regulatory policy makers have expressed increasing concerns about protecting Information and Communication Technology (ICT) systems as well as Industrial Control Systems (ICS)[26] from cyber-attacks. Many experts expect threats and attacks to increase in *"intensity & complexity"*[27] over the next several years. The OEB is unaware of any Ontario electricity customer data being compromised or of distribution system operations being impacted by successful cyber-attacks. Working with the IESO, the OEB continues to monitor and understand developments related to cyber security.

Cyberspace[28] has continued to expand beyond national borders, and its use and application by various entities have grown rapidly. Associated cyber risks are becoming more severe, widespread and globalised. Cyber threats have emerged as an urgent global challenge facing the international community as a whole.

Cyber-attack sophistication and the broadening of targets through various means are exponentially increasing the likelihood of an attack and breach. Small size does not necessarily minimise the risk any longer. Cyber hackers share their developments, and it is not uncommon for different individuals or groups to perform joint broad phishing campaigns from multiple jurisdictions through the use of a complex system of network hosts with large numbers of malicious files making repeated attacks against multiple servers inside a target. Protection from attack implies an ongoing need to secure resources with an up-to-date, evolving and in-depth understanding of the cyber world.

[26] 2016 - Congressional Research Service; Cybersecurity Issues and Challenges: In Brief: The act of protecting both Information and Communication Technology (ICT) and Industrial Control Systems (ICS) and their contents has come to be known as Cyber Security.
[27] 2015 – Fraser Institute; Cybersecurity Challenges for Canada and the US
[28] 2013 - Strategic Intelligence Management; p.215 - Cyberspace is an interactive domain made up of digital networks that are used to store, modify, and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.

Existing Regulatory Requirements

Distributors and transmitters through a number of existing legislative and regulatory requirements to ensure customers' personal information is protected and to incorporate security risk mitigation as part of their asset management plans. As discussed above, the OEB has also set out its expectations with respect to distributors and other regulated companies' need to address cyber security and privacy. Further, based on the statements in the Supplemental Report, the OEB has stated that it expects the industry to ensure it is meeting these responsibilities and adopting best practices to do so.

Privacy and security of customer data have always been a priority for the OEB as evidenced in licence conditions that were established with the original licences for electricity participants.[29] Security is about protecting and controlling information and the operating systems supplying energy to consumers. Privacy is about recognising that while distributors retain the physical control of the data, the decisions about how to collect, use and disclose personal information reflect the individual consent and personal preferences of consumers. The OEB has through licences and codes established requirements for the protection of consumer and other sensitive information.

Distribution Plans

The OEB's Filing Requirements for electricity distributors set out guidance and expectations to incorporate cyber security in distribution system plans:

> "…*showing the investment conforms to all applicable laws, standards and best utility practices pertaining to customer privacy, Cyber Security and grid protection…*" and
>
> "…*to justify projects/activities in this category should include but need not be restricted to a description of how advanced technology has been incorporated into the project (if applicable) and including how standards relating to interoperability and Cyber Security have been met…"*[30]

[29] 2013 - Report of the Board – Supplemental Report on Smart Grid (EB-2011-004) p.18
[30] 2013 – OEB Distribution System Plan - Filing Requirements for Electricity Transmission and Distribution Applications – Chapter 5, page 21 – Cyber Security, Privacy

Privacy Legislation

In developing the proposed framework the CSWG recognised that it must take into account existing privacy legislation. The Personal Information Protection and Electronic Documents Act apply to all privately owned regulated companies, while the Municipal Freedom of Information and Protection of Privacy Act applies to all Ontario municipal-owned electricity distributors.

Existing Cyber Security Environment

An environmental scan of cyber security practices and regulations was completed to assess the current standards, frameworks and regulatory approaches that might be leveraged to support the development of a cyber security framework for Ontario. The scan was also to identify agencies that may be undertaking cyber security activity at this time which could provide a basis for an approach in Ontario. The scan confirmed that standards and frameworks which focussed on the electricity distribution sector were at an early stage and not in a form that could be applied directly in Ontario. Below are the general observations from the scan:

- A number of practices and regulations exist for bulk and non-bulk operators within North America;
- Many appear generic in nature and have varying degrees of prescriptive requirements that need to be interpreted and applied to their operations; and
- A number of governmental agencies with varying degrees of regulatory authority have a mandate to develop cyber security strategies.

As discussed above, system operators of the bulk transmission systems are required to adhere to the established North American standards. Distribution accountabilities typically fall to states and provincial authorities. Distributor associations in the US have recognised the risks of cyber security attacks and have collectively invested heavily in procedures and guidelines for optional use by their members. Cyber maturity and capability reporting does not yet provide comparable results and is based on self-defined criteria set by the distributor and possibly its auditor.

All methodologies are missing tools or processes to support a consistent result in identifying a regulated entity's inherent risk, maturity level and auditing criteria. They require a good understanding of cyber risks, are subjective and not necessarily adaptable to smaller companies. During discussions regarding best practices in Ontario, it was evident that all are missing tools or supporting processes to fully leverage them for the development of this framework and achieve the OEB's mandate. Appendix D provides details on the results of the scan.

Foundation of the Framework

The White Paper provides the technical details and specifics of the proposed framework. This section of the Staff Report provides OEB staff's overview of the underpinnings of the proposed framework.

Based on insight from Industry Experts, the CSWG, and research into the various frameworks and industry standards, the NIST framework was chosen as the foundation for the proposed framework. It was adapted using specific insights from the US Department of Energy (DOE) Cyber Security Capability Model (C2M2)[31] and the Privacy by Design (PbD).[32]

The following provides the rationale for choosing the NIST Framework, the C2M2 Model and the PbD principles. Section 3 of the White Paper explains in detail how these elements have been adapted specifically for the proposed Ontario Cyber Security framework.

NIST

The NIST Framework is comprised of three elements: Framework Core,[33] Implementation Tier[34] and Profile.[35] The proposed framework uses only the NIST Framework Core. It relies on the C2M2 model for measurement and the PbD principles for privacy and data protection. As the framework evolves, the sector may choose to incorporate NIST's Implementation Tiers and Profiles as part of its proposed CSAC's activities.

NIST is a principle-based framework that is not prescriptive. It enables the integration of cyber security risk management into an organisation's overall risk management process and includes the ability to:

- Take into account the interaction of multiple risks;
- Address both traditional information technology (IT) and operational technology (OT);
- Encompass the entire organisation;
- Ensure that decision making is conducted internally by a risk-informed process of continuous improvement; and

[31] C2M2
[32] PbD 7 Foundational Principles
[33] NIST Framework Core Components
[34] NIST Framework Implementation Tiers; p.5
[35] NIST Framework Profiles; p.11

- Reference standards that can be used to support risk management activities.

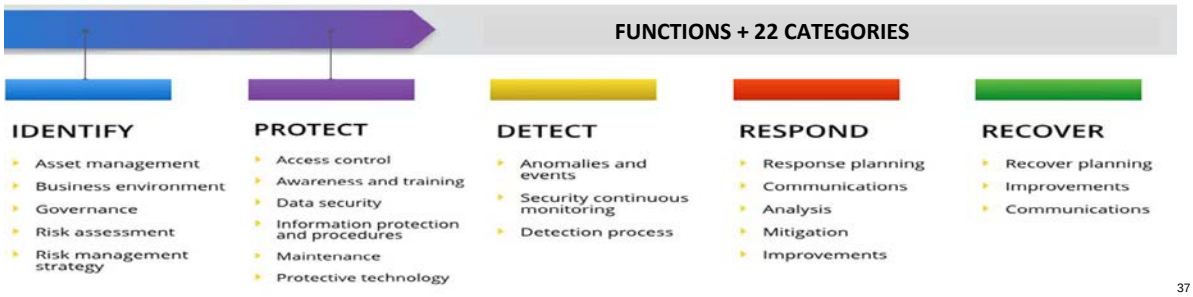
Functions

NIST is structured by core functions to provide a strategic view of an entity's risk management cycle. These core functions (*Identify, Protect, Detect, Respond, and Recover*) are the framework's fundamental "cornerstone" for how entities should approach their cyber security.

Categories

Each core function within NIST is further subdivided into *categories* which represent specific objectives to address each function. An example of a "*Protect"* related *category* would be, data security (PR.DS): information and records (data) are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information."[36]

The proposed framework includes the 22 NIST categories, as all were felt to have relevance to the sector's cyber security capability.



[37]

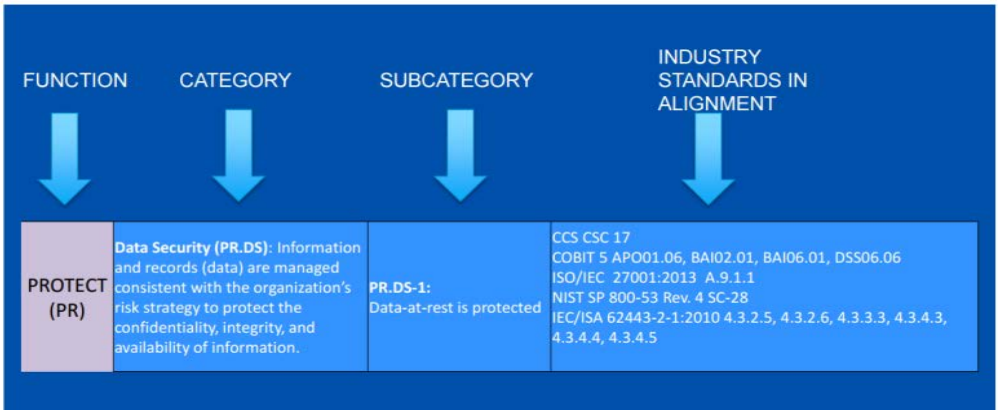
Sub-Categories

Supporting the 22 categories is a set of subcategories that represent specific, expected outcomes for work in each category. An example of a subcategory would be *"PR.DS-2 - Protect Data in Transit".*[38] One or more subcategories are mapped to each category. The current list of 98 subcategories in NIST has been pared down to focus on the most critical outcomes.

[36] 2014 - NIST Cyber Security Framework; p.19
[37] https://www.praetorian.com/nist/cybersecurity-framework
[38] Informative Reference: A specific section of existing standards and practices that are common among all critical infrastructure sectors and illustrate a method to accomplish the activities within each Subcategory. An example of an Informative Reference is ISO/IEC 27001 Control A.10 - Cryptographic technology, which supports the "Protect Data in Transit" Subcategory of the "Data Security" Category in the "Protect" function.

Standards and Guidelines Mapping

The proposed framework includes a mapping of many cyber security standards and guidelines to the NIST framework, and describes in detail what actions can be taken to support the outcome.[39] Distributors who have already invested significant effort into applying an alternate approach to cyber security can use this alignment to confirm whether they are meeting the outcomes expected. The mapping further serves to support distributors that are unsure of what actions need to be taken.[40]



NIST Benefits

Through the application of the NIST framework, distributors will be able to:

- Align functions, categories and subcategories with their business requirements, risk tolerance, and resources;
- Establish a roadmap for reducing cyber security risk that is well aligned with their goals; and
- Consider legal/regulatory requirements and industry best practices, and address risk management priorities.

NIST Limitations

As discussed earlier the OEB has set out an expectation that protection of consumer privacy is an obligation for all regulated companies. Currently, the NIST Framework does not include privacy in its guidelines.[41] In January 2017**,** NIST published a draft

[39] Appendix D - 2017- Ontario Cyber Security Framework White Paper
[40] 2014 – Chevron NIST Cyber Security Framework
[41] OEB staff note that NIST has reached out to the initiative to evaluate how privacy has been embedded into the Framework as they are in the process of remediating this gap.

report "Privacy Risk Management for Federal Information Systems"[42] (PRMF) for anticipating and addressing privacy risk.

Since the PRMF model is not yet fully developed, Privacy by Design (PbD) principles have been embedded into the proposed framework to address this limitation. Industry Experts and the CSWG concluded that it would be beneficial to incorporate the Fair Information Practice Principles (FIPP)[43] and PbD principles into the framework. PbD promotes inserting privacy and data protection into information technologies, organisation processes, networked architectures and entire systems of governance and oversight.[44]

Privacy requirements and controls have been applied to all risk levels.

C2M2

The C2M2 Program is a public-private partnership established as a result of the US Federal government's efforts to improve energy sector cyber security and to better understand the cyber security posture of the grid. C2M2 helps organisations, regardless of size, type, or industry, to evaluate, prioritise, and improve their own cyber security capabilities. The model was identified, organised, and documented by energy sector subject matter experts from both public and private organizations. It is comprised of three cyber security capability maturity models: cyber security capability maturity model (C2M2),[45] electricity subsector cyber security capability maturity model (ES-C2M2); [46]and the oil and natural gas subsector cyber security capability maturity model (ONG-C2M2).[47]

The C2M2 program is a voluntary evaluation process using industry-accepted best practices that can measure the maturity of an organisation's cyber security capabilities and is designed to measure both the sophistication and sustainment of a cyber security program. It is publicly available, applicable to distributors who are

[42] NISTIR 8062: An Introduction to Privacy Engineering and Risk Management in Federal Systems, Jan 2017
[43] The Fair Information Practice Principles (FIPP) were identified as eight (8) general principles that should be adhered to when collecting, using or disclosing personal information. As reflected in three key statutes, the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA), the Personal Information Protection Electronic Documents Act (PIPEDA), and the Freedom of Information Protection of Privacy Act (FIPPA). There is also a personal health information statute in Ontario, which is not applicable. Fair Information Practices Principles (FIPP): These principles are usually referred to as "fair information principles". They are included in the Personal Information Protection and Electronic Documents Act (PIPEDA), Canada's private-sector privacy law. Freedom of Information Protection of Privacy Act (FIPPA): The purposes of this Act are to provide a right of access to information under the control of provincial institutions in accordance with the principles that information should be available to the public, necessary exemptions from the right of access should be limited and specific, and decisions on the disclosure of government information should be reviewed independently of government. FIPPA takes into account privacy in determining whether information should be provided. FIPPA also provides individuals with a right of access to their personal information.
[44] PbD's Seven Foundational Principles *(Proactive, not Reactive; Privacy as the Default Setting; Privacy Embedded into Design; Full Functionality; Full Lifecycle Security; Visibility and Transparency; User-Centricity)* have been incorporated into the Framework.
[45] C2M2: Cybersecurity Capability Maturity Model (C2M2), Feb 2014
[46] ES-C2M2: Electricity Subsector Cybersecurity Capability Maturity Model, Feb 2014
[47] ONG-C2M2: Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model, Feb 2014

performing self-assessments and contains useful information including C2M2 facilitation guides and toolkits.

C2M2 was selected by the CSWG due to its relevance to the Ontario energy sector, as well as its approach to describing levels of maturity for various cyber security objectives and thus can be applied to the NIST framework. The C2M2 model allows distributors to categorise their operational and cyber risk management performance into one of four maturity indicator levels (MIL) during both normal operations and times of crises. The four MILs are described as follows:

- MIL0: Not Performed
- MIL1: Initiated, but may be ad hoc
- MIL2: Repeatable
- MIL3: Managed/Adaptive

The core objectives of adding the C2M2[48] to the proposed framework include: strengthening cyber security capability, enabling consistent evaluation and benchmarking of cyber security capabilities, sharing knowledge and best practices, enabling prioritised actions and guiding appropriate cyber security investments by CEOs.

Application of C2M2

The proposed framework has applied the C2M2[49] maturity levels to establish the benchmark[50] control objectives for each risk profile. Increased rigour (higher MIL levels) or additional MIL elements have been introduced for each NIST sub-category in the proposed framework to accommodate the various maturity levels. The proposed alignment of C2M2 to NIST is based on advice from the Industry Experts and discussions within the CSWG working sessions. The White Paper refers to this expectation as the *"initial achievement level.*"

The selected objectives are a starting point for the sector and distributors. It is expected that the requirements will be modified as the framework evolves to address the changing risk landscape. Distributors will also have reference mapping that can

[48] 2015 - SGIP- C2M2 and the NIST Cyber Framework;p.15
[49] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework – P.50-51 and P.57 and 62-63 – Initial Achievement Level (MIL) and C2M2 Maturity Integration Levels (MIL)
[50] Cyber risk benchmark is a standard or point of reference against which things may be compared or assessed. It will enable the OEB to increase its understanding of distributors risk and maturity in comparison to sector composite benchmarks.

be used to guide internal discussions regarding improvements beyond the benchmark objectives. As business risk rises, additional elements can be implemented to increase the overall maturity.

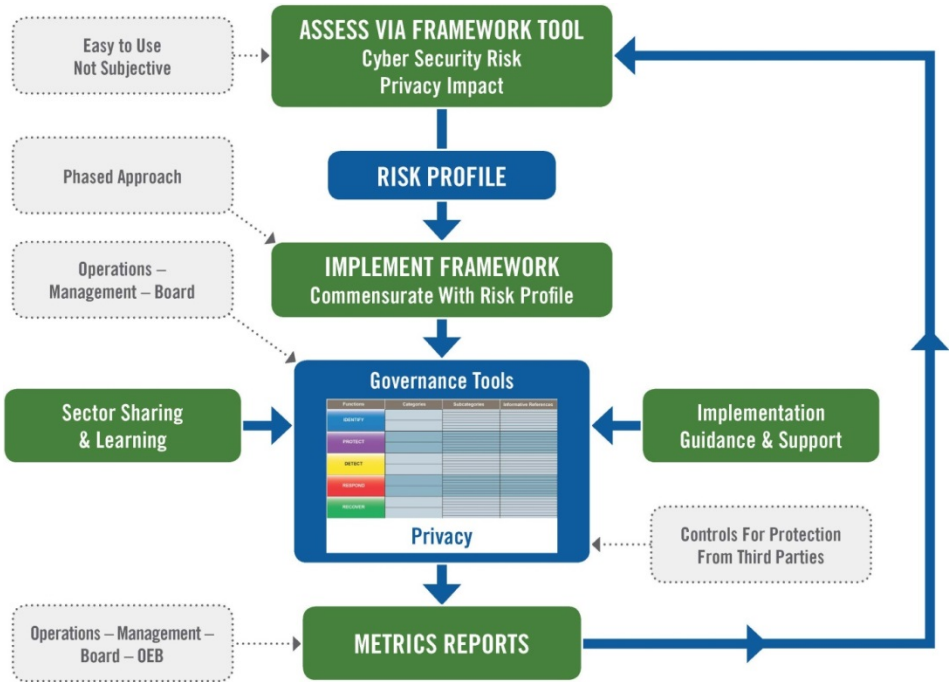
Ontario Cyber Security Framework

This section provides a general overview of the process and tools that are incorporated in the proposed framework. It highlights the tools and process-related activities developed and tested by the CSWG based on the objectives and criteria presented in previous sections. For more details on these tools and activities, see Section 3 of the White Paper.[51]

The framework incorporates best practices identified by industry:

- governance and risk management practices;
- reference standards, methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks;
- prioritised, flexible, repeatable, performance-based, approach, including security measures and controls, to help identify, assess, and manage cyber risks;
- tools for the identification of areas for including guidance for measuring performance; and
- Incorporate privacy requirements.

The following is an illustrative overview of the process and tools. A description of each stage of the process and the corresponding tools follow.



[51] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework

Proposed Framework Process and Component Descriptions

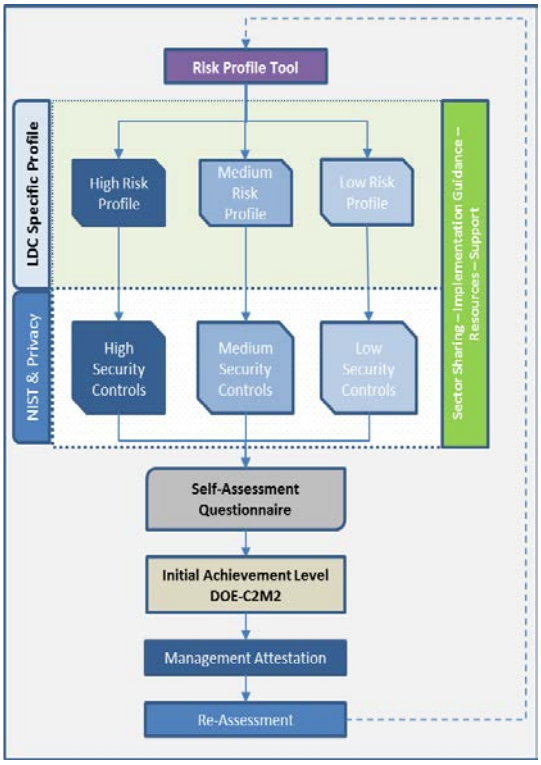
The proposed framework provides an industry-vetted methodology and toolset for assessing inherent risk, defining the benchmark objectives and measure progress toward those objectives. OEB staff expects that the application of this framework and associated toolset will help distributors, regardless of their size and current posture, identify gaps, prioritise and improve their cyber security capabilities and will enable a benchmark reference for assessing their cyber risk posture.

The CSWG noted that governance plays an extremely important role in achieving the security objective of the sector, not only for current needs but also for future challenges. The CSWG agreed that incorporating cyber security into the distributors' governance will elevate the understanding of cyber risk, and enhance business planning and risk management.[52]

Through the use of the framework, a maturity level and security gap report can be generated to provide senior leadership with a clear understanding of their current state of affairs and highlight any needs for further investments in cyber security.

Risk Profile Tool

The CSWG established 46 distributor related Risk Questions[53] and a weighting approach based on NIST that result in an objective, repeatable categorization of a distributor's cyber security risk level of ***low, medium or high***.[54] If a distributor feels that the benchmark is set too low for their overall business risk approach, they can increase their rating. OEB staff expects that after further experience with using this tool, the sector[55] will review the results and refine the questions and scoring.



[52] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; p.23-25, and 36.
[53] For more detail on how to utilize the 2017- Framework Risk Profile Tool please reference the 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; p.46-49
[54] Cyber security risk level are rated as either low (major investments in technology or special resources not required), medium (requires some technology or resources to address risk), or high (requires significant technology or resource investments to implement).
[55] Proposed sector led *Cyber Security Information Forum* (CSIF) action

Control Objectives

The CSWG worked with the Industry Experts to map the benchmark control objectives[56] that describe the strategic goals to mitigate the identified risks.[57]

The mapping creates a set of escalating controls differentiated by risk profile. The controls[58] are descriptive in nature, not prescriptive, and therefore allow the distributor flexibility in developing solutions that are aligned with their business practices.

The C2M2 model is incorporated into this step to provide additional details on the control activities that the distributor can implement.

The Industry Experts' assessment of the sector's existing use of NIST and C2M2 tools and processes determined that these processes offered the most guidance and were subsequently incorporated into the proposed framework. In effect, these processes can guide sector entities to apply effective controls that will assist in safeguarding their information, privacy and physical assets.

Similar to the proposed approach to risk scoring, the sector is expected to review the results from applying the control objectives and modify the controls accordingly.

The combination of risk level and mapped control objectives represent the target "Initial Achievement Level"[59] in cyber security that the distributors should be striving to meet. The distributor has complete flexibility in their approach to achieving the objectives.[60]

Self-Assessment Questionnaire (SAQ)

The SAQ is an additional tool developed by the CSWG to help distributors conduct effective evaluations of their cyber security practices against the control objectives. It is adaptable and scalable to distributor needs, goals, capabilities and environment.

---

[56] Control Objectives - Control objectives are the "aim or purpose of specified controls at the service organization which address the very risks that these controls are intended to effectively mitigate". control objectives are a series of statements put forth by an organization that address risks, for which these risks are to be effectively mitigated with supporting processes, procedures, policies, and related activities that are in place within the organization's control environment.
[57] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; p.47
[58] DOE RMP – C2M2 – Controls "The management, operational, and technical methods, policies, and procedures—manual or automated—(i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information."
[59] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; p.51 – Initial Achievement Levels
[60] Using the 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; Distributors (based on their existing maturity and posture) can leverage the 2017 - NIST Privacy Security Controls Self-Assessment Questionnaire (SAQ) and applicable control objectives to map their existing risk levels and asses the level of rigor required to achieve various maturity levels.

Through an interrelated set of questions, the SAQ[61] provides the opportunity to self-assess existing practices and approaches. For each subcategory, there is a choice of responses to indicate the distributor's status regarding a specific cyber security requirement.

The SAQ is a valuable tool for distributors to use in assessing and reporting the status of their cyber preparedness to their executive and Board of Directors.

Framework Continuous Improvement

The framework and the associated tools described above and detailed in the White Paper have been developed with extensive input from the CSWG. OEB staff and the CSWG recognize that the initial criteria, processes and tools will benefit from feedback based on the practical implementation of the framework. To further validate and enhance the framework's efficacy, and support continuous improvement, the CSWG recommended that a control group of distributors be selected to work with the industry experts, during the initial implementation. Through the use of this approach, identified gaps, necessary additional implementation guidance and refinements to the framework can be developed immediately and provided to all LDC's.

Third Party Independent Validation

Currently, distributors engage third parties to conduct penetration testing and validation of their cyber security preparedness. The application of the framework is expected to provide a sector-consistent approach and reference point for internal and independent security-specific audits.

The proposed framework (including the audit elements) is intended to serve as a common language for distributors to provide them with a mechanism for third party independent validation and reporting. Audits will enable the OEB and sector entities to leverage accredited 3rd party organisations (with core competencies in information security and control assessments) to undertake entity-wide cyber security examination engagements as trusted, independent assessors. OEB staff anticipates that future phases of the framework and the regulatory requirements may also require onsite audits by accredited (3rd party) firms.

[61] For more detail on how to utilize the 2017 - NIST Privacy Security Controls Self-Assessment Questionnaire (SAQ) please reference 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; p.54 and 55

Governance Model

The CSWG discussed and noted that governance plays an extremely important role in achieving the security objective of the sector, not only for current needs but also for future challenges. In the absence of a recognised sector specific standard or framework, it is not possible to consistently address and report on cyber security risks.

By the sector establishing a common framework for a consistent approach and criteria, it provides the basis for assessment and reporting that can be compared. CSWG agreed that incorporating cyber security into the distributors' governance will elevate the understanding of cyber risk, and enhance business planning and risk management.[62] Through the use of the framework, a maturity level and security gap report can be generated to provide senior leadership with a clear understanding of their current state of affairs and highlight any needs for further investments in cyber security.

Certification Model

From the research by the Industry Experts, OEB staff has noted that high-performing entities who have already adopted a self-reporting certification model[63] are better able to mitigate risks, vulnerabilities and attacks, and continue to improve their cyber posture. Towards achieving a consistent and repeatable assurance, OEB Staff is proposing that the OEB require the distributors to certify their cyber security capability, against their inherent risks. In order to provide cogent reporting that the OEB will be able to rely on, OEB staff suggests it should be based on the framework unless there are reasons to deviate from that basis.

The typical planning and certification model[64] includes the following steps:

- Determine Risk Profile: Periodically assess the level of risk that is inherent in the business through the use of objective and subjective approaches**;**
- Assess: Periodically assess the security controls in organisational information systems to determine if the controls are effective in their application;
- Develop: Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organisational information systems;

[62] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework; p.23-25, and 36.
[63] 2017 - Ontario Non-Bulk Energy Sector Cyber Security Framework;4.2 - Reporting
[64] 2011 - NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations; p.11

- Authorise: Authorise the operation of organisational information systems and any associated information system connections;
- Monitor: Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls; and
- Report: Report status of overall progress to achieve compliance to control objectives, and support certification reporting to the OEB.

Framework Implementation

Regulatory Amendments

In order to implement the framework, OEB Staff is recommending that the OEB require mandatory participation in the proposed *Cyber Security Information Forum (CSIF)* to promote industry awareness and training. Full participation by all distributors in the CSIF will, in staff's view, deliver the greatest value to the sector and provide assurance to the OEB that all distributors are taking the necessary actions to improve their cyber posture.

In its Supplemental Report on Smart Grid, the OEB stated its expectation that the industry would lead to the development of standards for privacy and cyber security. OEB staff has taken on the role of facilitator to develop the proposed framework and build awareness in the sector. Going forward, for the sector to be successful it must own the framework and ensure it evolves to address new challenges and risks. Staff, based on the advice of the CSSC and CSWG is recommending the establishment of a sector-driven Cyber Security Advisory Committee. This approach is similar to the EBT Standards[65] and Regional Planning Advisory Committees[66] ensuring sector accountability for the framework and its evolution.

Interim Reporting

As part of a risk-informed approach to cyber security certification and the importance of early indication that industry is taking appropriate measures to establish a cyber security posture consistent with their risk assessment; OEB staff recommends that there be a regulatory requirement to certify cyber security and privacy.

To provide the OEB assurance that the Framework is being worked on, OEB staff is recommending that industry provide an initial report[67] within three (3) months after the framework is issued acknowledging that it:

- *has reviewed and understood the framework;*
- *has taken steps to plan and implement compliance;*
- *has assigned a team to assess risk and their current capability in implementing the framework objectives to achieve such compliance;*

[65] 2003 – Electronic Business Transaction (EBT) Standards (RP-1999-0032)
[66] 2011 – OEB - Regional Planning for Electricity Infrastructure (EB-2011-0043)
[67] Please reference Appendix E – Interim Report.

and

- *confirmation they will furnish an annual certification of compliance.*

Annual Reporting

Further, OEB staff proposes that distributors should be required to "certify" their cyber security status relative to the benchmark objectives and timeframes to achieve compliance within twelve (12) months after the issue of the framework.

OEB staff recommends an annual certification of compliance be submitted to the OEB by each distributor, in order to provide assurance of the licenced entity's cyber security capability and that the assessment has been against the framework to provide a consistent reporting across the sector.

Within twelve (12) months of the issuance of a final framework, distributors would be expected to:

- *Determine their Risk Profile;*
- *Understand the control requirements;*
- *Assess current cyber readiness;*
- *Assess Effectiveness of Security Controls;*
- *Develop and Implement plans of action to remediate deficiencies;*
- *Conduct Monitoring of Information System Security Controls (ongoing) and reduce vulnerabilities; and*
- *Provide to the OEB, an annual certification[68] confirming the above in meeting those cyber security objectives.*

Accordingly, cyber security investments and actions should continue to be incorporated and aligned within distribution plans and support the evaluation criteria associated with cyber security and Privacy.[69]

---

[68] Certification: Distributors should periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; authorize the operation of organizational information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. A sample of the proposed self-certification document is attached. Please reference Appendix B - Self Certification Example.

[69] 2013 – OEB - Consolidated Distribution Systems Plan Filing Requirements, Chapter 5, Section 5.4.5.2 B 3

OEB staff proposes that a compliance plan supporting the annual certification[70] reporting provides a strategic view of the longer term approach to cyber security while providing short-term reporting and monitoring of progress.

Developing the Supporting Infrastructure

The framework is a living document and will need to be continually updated as best practices, authoritative reference methodologies and industry experience and knowledge expand. The CSWG and the CSSC both recommended a CSAC be established, noting that this committee would be vital to maintaining the framework and improving the ongoing cyber security capability within the sector. OEB staff supports this sector approach and is proposing to facilitate the establishment of the CSAC. OEB staff also proposes to initiate discussions with the CSAC, once it is established and other stakeholders on the development and proposed mandate of the CSIF. Early thinking from the CSSC and CSWG suggest that the CSIF will play a key role to:

- Improve awareness of the cyber security risk;
- Enable sector-wide sharing of actionable responses to cyber incidences;
- Enhance sector sharing and learning;
- Provide insight to the development of the Sector Guidebook; and
- Engage with other associations,[71] to share best practice to build awareness and knowledge in cyber security.

CSWG also recommended that all confidential distributor information and data shared in the CSIF would be anonymous within this sector-led group. OEB staff is of the view that participation in this CSIF is to be mandatory.

[70] Reference - Appendix B; proposed Certification Sample
[71] Potential associations may include: APPA, NRECA, NIST, EPRI etc.

This Page Kept Intentionally Blank

Appendix A – Participants

An extensive number of executives, experts and policy makers participated in the projects' workshops and expert interviews throughout 2016. OEB staff would like to thank the members of the Cyber Security Steering Committee and Cyber Security Working Group Members for providing their thoughtful insights and advisory efforts in relation to developing the proposed Cyber Security framework. OEB staff is deeply indebted to all of those who have provided their valuable thought-leadership and expertise to this framework's development.

Cyber Security Steering Committee Members (CSSC)

Hydro One	Gowling WLG (Canada) LLP
Toronto Hydro	IESO
Oshawa PUC	EDA
Enbridge	University of Toronto
Hydro Ottawa	North Bay Hydro
PowerStream[72]	

Cyber Security Working Group Members (CSWG)

Horizon Utilities	IESO	Oakville Hydro
Oshawa PUC	Hydro One	Thunder Bay Hydro
EnergyPlus	PowerStream	London Hydro
Waterloo North	Toronto Hydro	Ministry of Energy
Enersource	Hydro Ottawa	Peterborough Hydro
Veridian	Burlington Hydro	Entegrus
EDA	Enbridge	Union Gas
Electrical Safety Authority	Orangeville hydro	Halton Hills Hydro
	Renfrew Hydro	

[72] 2017 - Alectra Utilities Corporation - formed by the merger of the municipally-owned utilities Enersource (Mississauga), Horizon Utilities (Hamilton and St. Catharines), and PowerStream (York Region and Simcoe County).

Appendix B – Self-Certification Example

Cyber Security Framework Certification

(Confidential)

Ontario

Date:

Based on the results noted in the SAQ dated *(completion date)*, the signatories identified below assert the following compliance status for the entity as of *(date)*: (***check one):***

Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

☐ **Compliant:** All relevant sections of the SAQ are complete, all questions answered affirmatively, resulting in an overall COMPLIANT rating; thereby *(LDC Name)* is in full compliance with the Cyber Security framework.

☐ **Non-Compliant:** Not all sections of the SAQ are complete, or not all questions are answered affirmatively, resulting in an overall NON-COMPLIANT rating, thereby *(LDC Name)* is not in full compliance with the Cyber Security framework.

Target Date for Compliance: [Date]

☐ **Compliant but with Legal exception:** One or more requirements are marked "No" due to a legal restriction that prevents the requirement from being met.

If checked, complete the following:

Affected Requirement	Details of how legal constraint prevents requirement being met

☐ If my environment changes, I recognise I must reassess my environment and implement any additional Cyber Security framework requirements that apply.

☐ Cyber Security framework Self-Assessment Questionnaire (Low/Medium/High), Version *(a version of SAQ)*, was completed according to the instructions.

☐ All information within the above-referenced SAQ and in this certification fairly represents the results of my assessment in all material respects.

☐ I have read the Cyber Security framework and I recognise that I must maintain compliance, as applicable to my environment, at all times.

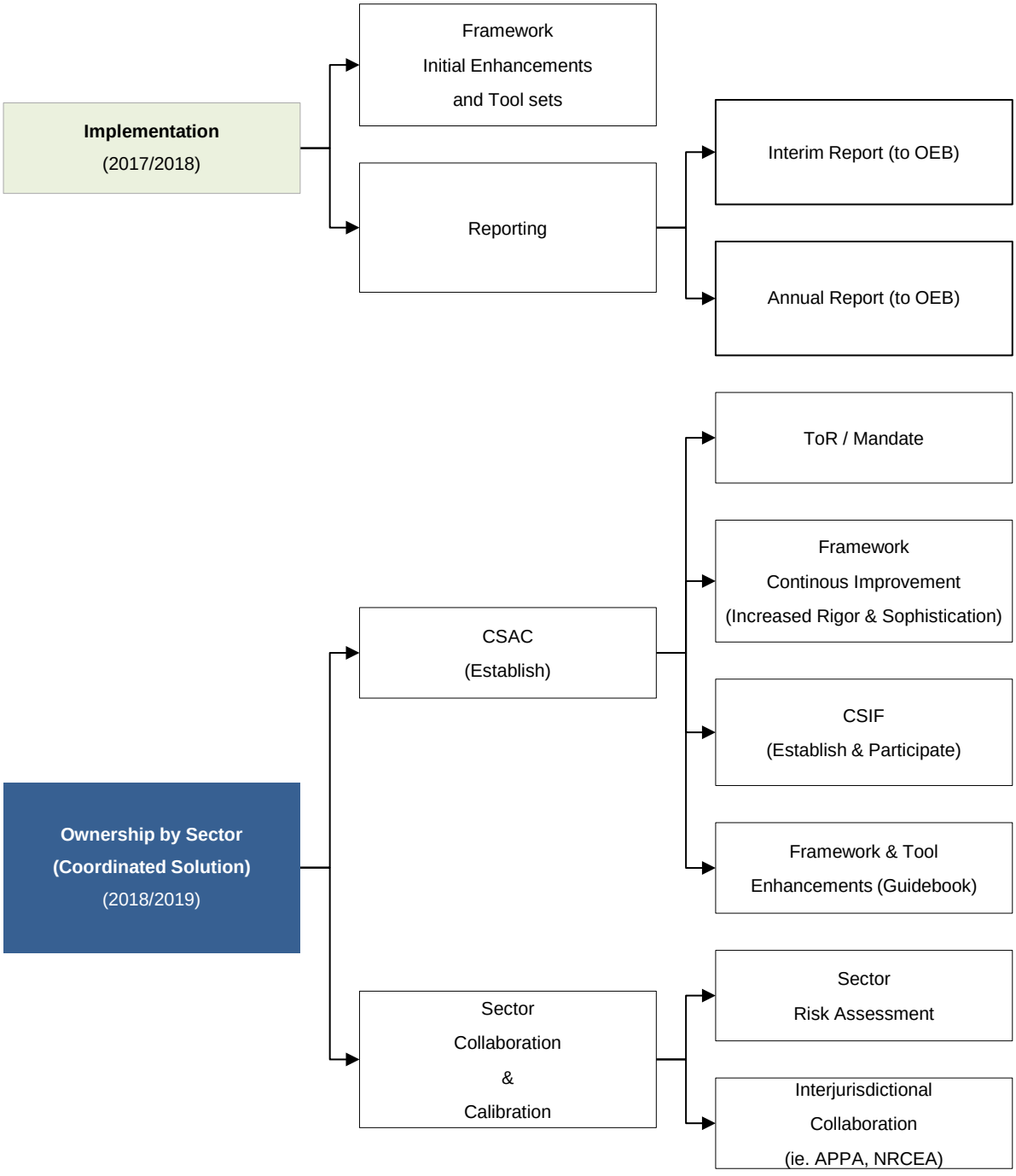
Certification

Signature of Licensee Executive Officer *Date:*

Licensee Executive Officer Name: *Title:*

Appendix C – Next Steps Flowchart

As noted throughout this Staff Report, additional work, by distributors is required pre and post implementation of the framework. Below is a mapping that illustrates the various streams of the planned activities.



Appendix D – Existing Cyber Security Environment Scan

The following provides an overview of agencies that are currently involved in cyber security with respect to the energy sector.

Canadian Cyber Security Agencies

In Canada, a combination of federal, provincial and local authorities have shared jurisdiction over cyber security. Canada's national strategy was developed in 2010 and includes partnering to secure vital cyber systems outside of the federal government. Through this objective, specific initiatives for the Government of Canada to partner with provinces along with the private sector were identified.

A review of legislation and regulatory requirements by energy regulators in Canadian provinces and territories was conducted in 2016. While several jurisdictions are considering the development of cyber security requirements, OEB staff did not identify any specific regulatory requirements as being in place at this time.

Public Safety Canada (PSC)

In Canada, Public Safety Canada (PSC) has the responsibility for Canada's Cyber Security Strategy, including partnering with critical infrastructure sectors. It has produced a Canadian version of the NIST standard. PSC has established the Canadian Cyber Incident Response Center (CCIRC)[73] for information sharing and incident response.

Canadian Cyber Incident Response Centre (CCIRC) is Canada's national coordination centre responsible for reducing the cyber risks faced by Canada's key systems and services. It is anticipated that CCIRC will see a "significant" increase in its ability to respond to, and mitigate, cyber incidents in the private sector, including the development of real-time automated feeds of cyber threat information that will give the private sector additional threat information and faster dissemination.

National Energy Board (NEB)

At a federal level, the National Energy Board **(**NEB) verifies regulated companies have adequate security to deter, respond to and manage security threats, including criminal and terrorist activity. The NEB mandate also includes the promotion of

[73] Public Safety Canada

security awareness, communication and information sharing among regulated companies. NEB-regulated companies are required to have an adequate, implemented and effective security program that meets CSA Z246.1 (Security Management for Petroleum and Natural Gas Industry) which is described below.

Technical Standards Safety Authority (TSSA)

The TSSA which has responsibility for the safety of among other things oil and gas pipelines in Ontario, including natural gas distributors' systems, has also adopted the CSA Z246.1. TSSA has indicated that all natural gas distributors have adopted this standard through the Oil and Gas Code Adoption Document.[74]

IESO and the Ontario Bulk Electricity System (BES)

As indicated above the IESO is responsible for compliance with NERC CIP in Ontario. To support compliance with this standard, in 2013, the IESO initiated the development of a provincial, collaborative, open and voluntary Forum.[75] Today, a growing number of distributors, as well as other sector participants, are actively engaged in this forum where information can be shared and awareness of cyber security is enhanced.

Provincial Regulatory Cyber Security Oversight (Electricity)

A cursory review of legislation and regulatory oversight pertaining to cyber security for energy in Canadian provinces and territories was conducted in 2016. The research was handled through an evaluation of the websites for each jurisdiction's regulatory bodies and professional associations. Several jurisdictions are considering the development of requirements; however, nothing is in place.

International Agencies and Activities

The European Commission has established a cyber-security proposal (NIS Directive)[76] to be implemented in 2017 with expectations that entities are properly equipped to respond to cyber-attacks through a computer security incident response team.[77] It is strategic in nature, and member states are expected to co-operate and support a culture of security across sectors.

[75] IESO Forum
[76] NIS Directive
[77] CSIRT Network

The "Basic Cyber Security Basic Law"[78] requires that the government of Japan establish uniform cyber security standards and obligates businesses related to critical infrastructure to take voluntary measures to enhance cyber security and co-operate with the government to implement relevant measures.

In the United States, the Department of Homeland Security, through the S.754 Cybersecurity Information Sharing Act, 2015,[79] is responsible for protecting the critical infrastructure of the United States from physical and cyber threats. Amongst a number of activities, it established the National Cyber Security and Communications Center that analyzes cyber security information, shares actionable information and coordinates response mitigation and recovery efforts at the national level. It does not set standards but does establish requirements and provisions for incorporating security controls and alignment to common sets of security standards and security practices.[80]

Additionally, the Federal Energy Policy Act of 2005[81] applies to the bulk electricity sector that falls under the jurisdiction of the Federal Energy Regulatory Commission (FERC). As described earlier NERC, under the direction of FERC, has established the CIP standards.

Distributor Associations

OEB staff has learned through its outreach that the American Public Power Association (APPA) and the National Rural Cooperative Association are actively collaborating on cyber security issues. The APPA, an organisation of more than 2,000 community-owned electric utilities established the Cyber Security and Physical Preparedness Committee (CAPP), a collection of APPA members who serve on working groups and share information related to security issues. APPA and its members also participate in the Electricity Subsector Coordinating Council (ESCC), a government/industry partnership focused on security and information sharing. As noted in the White Paper, APPA is planning to support its members by developing a cyber security framework similar to the OEB policy initiative.

The National Rural Electric Cooperative Association (NRECA[82]) is the national service organisation for more than 900 not-for-profit rural electric cooperatives and

[78] 2014 – Japan: Cyber Security Basic Act
[79] 2015 - S.754 – Cyber security Information Sharing Act of 2015
[80] DHS (Sec. 205) must issue binding operational directives to assist the OMB in ensuring timely agency adoption of and compliance with standards for securing agency information systems. (Sec 405) HHS must collaborate with DHS, health care industry stakeholders, NIST, and other entities to establish a single, voluntary, national, health-specific cyber security framework with a common set of standards and security practices as a resource for cost-effectively reducing cyber security risks for health care organizations.
[81] FERC

public power districts. Its members include consumer-owned, local distribution systems (the vast majority) and 66 generation and transmission (G&T) cooperatives that supply wholesale power to their distribution cooperative owner-members. The Cooperative Research Network (CRN)[83] forms part of NRCEA who performs collaborative research, development, demonstration and implementation of advanced technologies, methods and information to support the interest of the electric cooperatives, including a focus on cyber security.

Existing Frameworks and Standards

AESI identified best practices that could be applied to the Ontario energy sector. To do this, AESI surveyed Ontario distributors and researched cyber security in other sectors (i.e. Financial, Utilities, Energy, Technology and Retail).

The survey revealed in order to assess cyber security Ontario electricity distributors are using NERC CIP as well as a variety of frameworks and standards which are described below.

National Institute of Standards and Technology Framework (NIST CSF)

NIST has developed a broad Cyber security Framework (NIST CSF) [84] that enables the integration of cyber security risk management into the organisation's overall management process. This framework is generic in nature, allowing for a significant amount of flexibility and interpretation. It appears that this standard is becoming the leading methodology used by many critical infrastructure entities. The NIST framework is a bottom-up approach to enhancing privacy-sector cyber security. Less complex than other cyber security frameworks, it is intended to remain flexible, voluntary and cost-effective.[85]

Electricity Subsector Cyber Security Capability Maturity Model (ES-C2M2)

The Electricity Subsector Cyber security capability maturity model[86] is a program developed in a public-private partnership to improve the electricity subsector cyber security capabilities and to understand the cyber posture of its entities. It is a voluntary evaluation process utilising industry-accepted cyber security practices that can be used to measure the maturity of an organisation's cyber security capabilities and is designed to measure both the sophistication and sustainment of a cyber

[84] 2014 – NIST- Cyber Security Framework
[85] 2016 – Bottoms up: A Comparison of "Voluntary" Cyber Security Frameworks
[86] C2M2

security program. However, C2M2 is very sophisticated, highly complex, comprehensive and difficult to use without subject matter expert's involvement.

North American Electricity Reliability Corporation (NERC CIP)

The North American Electric Reliability Corporation[87] critical infrastructure protection plan targets critical bulk transmission system assets that impact interoperability and system interties[88] in North America.[89] These mandatory standards, enforceable for bulk transmission systems, focus on performance, risk management and entity capabilities. NERC CIP is a mandatory[90] and enforceable reliability standards; subject to NERC Commission review and approval. They are robust and under continuing development; CIP standards are highly onerous to implement and very expensive to achieve compliance.

ISO/IEC 17799, 27000, 14001

ISO/IEC 17799, 27000 and 14001[91] is a series information security standards developed by the International Standards Organization to provide a broad information framework that can be applied to various types and sizes of organisations. ISO/IEC standards are highly complex and are being applied and implemented by a few distributors voluntarily. The ISO/IEC standards are more flexible in terms of scope, controls, compliance, and enforcement and designed to be applicable to a variety of organisations. The standard is voluntary; distributors may decide which controls are applicable.

Control Objectives for Information and Related Technology (COBIT)

COBIT[92] is a framework for developing, implementing, monitoring and improving information technology (IT) governance and management practices. Published by the IT Governance Institute and the Information Systems Audit and Control Association (ISACA) it is a good practice guide (toolset) created by international professional association ISACA[93] for information technology (IT) management and IT governance and was considered as a candidate to be applied to the sector.

---

[87] Critical infrastructure protection (CIP) is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. The US Department of Homeland security has identified 16 critical infrastructure sectors of which electricity is one.
[88] 2014 - IESO - Intertie Report
[89] 2012 - Ministry of Energy - Hydro One Networks has 27 interconnections with other utilities at 345,000, 230,000, 115,000 and 69,000 volts. This number includes nine interconnections with New York; ten will Québec, four with Michigan, and three with Manitoba and one with Minnesota. The term "Interconnection" means a geographic area in which the operation of bulk-power system components is synchronized such that the failure of one or more of such components may adversely affect the ability of the operators of other components within the system to maintain reliable operation of the facilities within their control.(16 U.S. Code § 824o - Electric reliability.)
[90] Section 215 - Federal Power Act (FPA)
[91] ISO Standards
[92] COBIT
[93] ISACA – Information Systems Audit and Control Association

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is the Payment Card Industry Data Security Standard[94] which sets the standards for the protection of payment card data. Distributors that use this method of payment are required to comply with this standard. PCI is internationally recognised, voluntary in compliance, possessing a high degree of flexibility in its application. Controls are much more strict and specific. Companies (generally financial in nature) must comply. The strictness[95] of the PCI DSS makes it difficult for organisations to become fully compliant.

Federal Financial Institutions Examination Council (FFIEC)

FFIEC[96] is a formal U.S. government interagency body composed of five banking regulators who developed the "Cyber Security Assessment Tool" (Assessment) to help institutions identify their risks and determine their cyber security preparedness. Use of the risk assessment process and tool is a voluntary[97]. It is highly complex and was designed specifically for the financial sector. AESI and the CSWG reviewed the Assessment Tool and decided it would not be appropriate for the Ontario energy sector as it is targeted for a mature entity or sector.

Security Management for Petroleum and Natural Gas Industry Systems (CAN/CSA Z246.1)

Published in 2009, by the CSA Group[98], CSA Z246.1[99] was developed to be scalable, enabling it to be used by both small and large operating companies. This National Standard specifies criteria for establishing a Canadian security management program for petroleum and natural gas industry systems to ensure security threats and associated risks are identified and managed. Provides requirements for a continuous improvement process to develop, implement, maintain, and evaluate an emergency preparedness and response program. This standard provides mitigation and response processes and procedures to prevent and minimise the impact of security incidents that could adversely affect people, the environment, assets, and economic stability. Compliance is assured through audits of the operator's procedures, manuals and programs. The frequency of inspections and audits vary. Their security management program is based on factors such as type, size, location

[94] 2004 - PCI
[95] 2010 -Compliance Standards in Data Security
[96] 2015 - FFIEC
[97] 2016 - FFIEC Cybersecurity Assessment Tool
[98] 2014 - CSA
[99] 2009 – CAN/CSA - Z246.1- Security management for petroleum and natural gas industry systems. CSA Z246.1 provides a framework to protect energy infrastructure from malicious damage through risk-based and performance-based management processes.

and criticality of the assets being protected and companies will make decisions based on their internal assessment of risks related to their facilities.

> *"…this Standard uses the concept of a security management program, and in particular risk management, to address security issues. This Standard provides a performance-based approach for use by the operator to establish governance, conduct planning, implement and improve security operations (including detection and mitigation practices), and refine the security management program through change management and audit processes. This approach allows users to apply this Standard across the petroleum and natural gas industry…."*[100]

This standard is applied to natural gas pipelines through the authority of Ontario's Technical Standards and Safety Authority (TSSA) and applies to all onshore petroleum and natural gas industry systems.[101]

[100] 2016 - CSA-Z246.1-13 - Security management for petroleum and natural gas industry systems
[101] 2016 – CSA; Section 1.3 – standard does not apply to offshore petroleum and natural gas platforms.

Appendix E –Interim Report Example

Cyber Security Framework Interim Report

(Confidential)

Ontario

Date:

Based on the results dated *(completion date)*, the signatories identified below assert the following interim report for the entity as of *(date)*: (***check one):***

Acknowledgement of Status

Signatory(s) confirms:

(Check all that apply)

- ☐ I have read, reviewed and understood the Cyber Security framework and I recognise that I must maintain compliance, as applicable to my environment,.
- ☐ I have assigned a team to assess risk and their current capability in implementing the framework objectives to achieve compliance.
- ☐ I have prepared an interim plan to certify and confirm I will furnish an annual certification of compliance.
- ☐ I have taken steps to plan and implement compliance with Cyber Security framework requirements that apply.

Interim Report Acknowledgement

Signature of Licensee Executive Officer *Date:*

Licensee Executive Officer Name: *Title:*