ONTARIO ENERGY BOARD

Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario – Cyber Security Framework

Assessment Report on the Cyber Security Framework and Implementation

As the supporting consultant, AESI Acumen Engineered Solutions International Inc. prepared this report on behalf of the Cyber Security Working Group.

December 31, 2017

775 Main Street E
Suite 1B
Milton, Ontario
Canada L9T 3Z3
P · 905.875.2075
F · 905.875.2062

www.aesi-inc.com

TABLE OF CONTENTS

1. Introduction and Objectives of Report 1

2. Summary of Feedback Related to Industry Implementation of the Framework 3

2.1. Summary of Stakeholder Feedback from the Comment Period 3

2.2. Summary of Feedback from the Focus Groups 5

2.2.1. Framework Tools 5

2.2.2. Implementation 7

3. Attaining the Initial Achievement Levels 8

4. Recommendations for Industry Implementation of the Framework 9

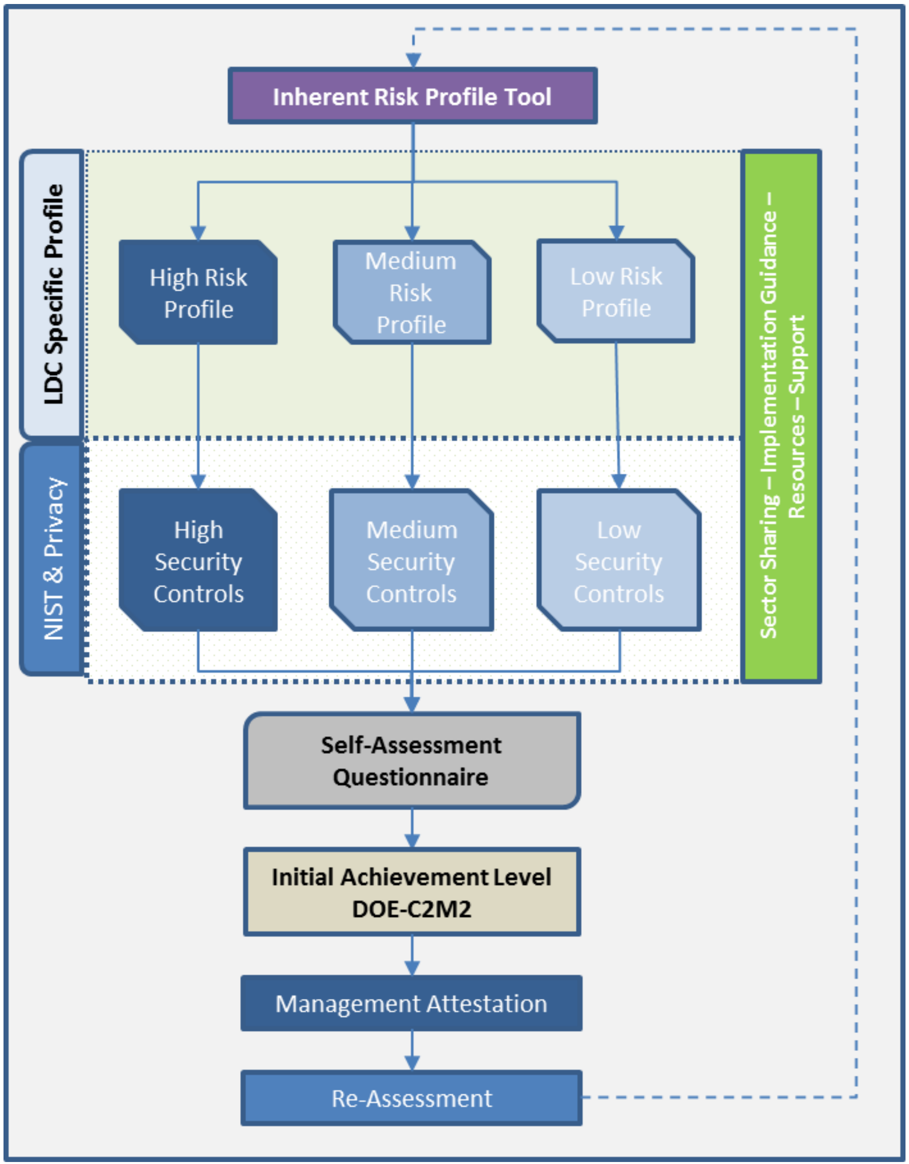
Appendix A: Glossary of Terms and Abbreviations 11

1. Introduction and Objectives of Report

This Report has been commissioned by the Ontario Energy Board (EB-2016-0032) to consolidate the Cyber Security Working Group's (CSWG) work to finalize the Framework and aid in the implementation of the proposed industry Cyber Security Framework (Framework). The objectives of this report are to summarize industry stakeholder feedback to date, to provide proposed changes to the Framework tools, and to provide guidance for the effective implementation of the Framework by the industry.

Through extensive iteration with the Cyber Security Steering Committee (CSSC) and the Cyber Security Working Group (CSWG), using both qualitative and quantitative research methods, the Consultant Team (AESI Inc., DLA Piper and Richter) developed an Ontario specific Cyber Security Framework applicable to any Local Distribution Company (LDC, also referred to as "distributors") or transmitter of non-bulk assets in Ontario. The Cyber Security Framework uses the NIST Cybersecurity Framework as the cornerstone of the Framework and includes insights from the Department of Energy (DOE) - Cybersecurity Capability Maturity Model (C2M2)[1], Privacy by Design (PbD), and input from a wide variety of stakeholders. Conceptually, the Cyber Security Framework can be visualised as seen in Figure 1.

Figure 1: Ontario LDC Cybersecurity Framework, Stage 1



[1] Cyber Security Capability Maturity Model (C2M2) Program

The Cyber Security Framework process begins with a Risk Profile Tool developed with input from the Cyber Security Working Group (CSWG) and was specifically tailored to the inherent risks in Ontario's LDC community. The Risk Profile Tool allows each Ontario LDC to be categorised based on their inherent risk, in an objective fashion. Based on size, maturity and capability, Ontario LDCs will have different inherent risk profiles. Each risk profile will require that varying degrees of security controls be applied to ensure an adequate level of confidence in the entity's cybersecurity posture.

Once a risk profile for the LDC is established using the tool, the LDC would reference the recommended set of security and privacy controls (based on the NIST Cybersecurity Framework[2], with the injection of PbD) that are defined for High, Medium and Low (considered as "baseline") Risk entities.

To aid in the development of this report a subset of the CSWG was established in focus group format, and their recommendations were accepted by the CSWG in whole, and are included in this report.

[2] Cyber Framework

2. Summary of Feedback Related to Industry Implementation of the Framework

2.1. Summary of Stakeholder Feedback from the Comment Period

The comment period on the CSWG proposed Framework, implementation recommendations (White Paper) and supporting documentation yielded excellent feedback from the Stakeholders on the implementation of the Framework. Four key themes emerged: support, industry alignment, timing and cost. This feedback from the Stakeholders is summarized in the table below by the key themes.

Category	Summary of Comment Period – Stakeholder Feedback Related to Implementation
Support	• Recommend formation of a Cyber Security Advisory Committee (CSAC) that would be tasked with guiding the implementation of the Framework and developing the mandate of a Cyber Security Information Sharing Forum (CSIF). • Recommend that the CSIF be an open forum in which market participants can share technical, strategic, and intelligence information. Note: sector sharing and support was discussed in the White Paper released on June 1, 2017.[3] • Recommend coordination of electricity and natural gas efforts including the Canadian Cyber Threat Exchange (CCTX) and applicable Information Sharing and Analysis Centers (ISACs) • Request clarification of the Centralized Compliance Authority discussed in the White Paper. • Recommend leveraging existing industry forums (IESO, NERC E-ISAC, etc.). • Request clarification of audit criteria and third party certification. • Recommend provision of additional tools and guidance. • Request clarity of development of Key Risk Indicators (KRIs). Note: these were described in the White Paper. • Request sector maturity data and market analytics.
Alignment	• Recommend alignment to standards vs adapting standards. Note: the Informative References shown in the NIST Cybersecurity Framework lists the standards applicable for each security control. • Recommend alignment with the Bulk Electric System (BES) and ensure that strategies are in place to address the gaps across systems. • Recommend alignment with natural gas stakeholders via a cyber security task force. • Recommend that physical security measures are not overshadowed by this initiative. • Recommend further investigation and consideration of protection of consumer information. • Recommend close alignment with vendors.
Timing	• Recommend advancement at a measured pace to allow for lessons learned and insights to be accumulated. • Request clarity on timing of implementation and compliance details. • Request clarity on transition from Stage 1 to Stage 2.
Cost	• Suggest that costs and cost effectiveness should be taken into account in the implementation of the Framework. • Recommend a sector-wide financing arrangement for funding of cyber security initiatives. • Recommend a universal deferral account for distributors to use to record the costs to achieve compliance. • Recommend that physical security costs are shown with the cyber security costs in the rate application process. • Suggest potential for vendor funding.

[3] "White Paper: Cybersecurity Framework", Ontario Energy Board, June 1, 2017

2.2. Summary of Feedback from the Focus Groups

2.2.1. Framework Tools

The Focus groups reviewed in detail the Inherent Risk Profile Tool and the Security Controls spreadsheet. The following summarizes the changes to the Inherent Risk Profile Tool from the Focus group members:

INHERENT RISK PROFILE TOOL REVISIONS FROM THE FOCUS GROUP

Question Number	Question Area	Revisions
3	Employees and subcontractors that work remotely	Revised additional context "This includes anyone working from home or remote offices, and accesses utility networks remotely (e.g. using a VPN or similar connection)".
8	Processing credit card transactions or pre-authorized bank payments	Adjusted responses to be "Yes – On-Site Client Data" (3 pts), "Yes - NO Onsite Data" (0 pts), "No" (0 pts)
14	Third parties that have access to LDC systems	Adjusted text in selection to avoid displaying formatting error message (changed "10-50" to "10 to 50")
22	Smart Energy Technology	Revised additional context "This refers to devices at customer sites that communicate usage information to the utility such as smart thermostats, Home Area Networks, etc."
22	Smart Energy Technology	Adjusted text in selection to avoid displaying formatting error message (changed "10-50" to "10 to 50")
30	Remote administration of field devices	Adjusted question - added "operational" before "field devices"
34	Wireless communication networks	Revised additional context "Wireless includes all forms of wireless including proprietary, WiMAX, microwave, etc. Any wireless access is a potential external access point to systems."
39	Off-site data storage	Revised question "Do you allow sensitive data to be stored offsite?"
n/a	Thresholds for Medium and High-Risk ratings	Added +/- 10% transition bands for total risk scores to transition from Low->Med (63-77) and Med->High (108-132)

The most significant change is the addition of a ranged threshold to transition between the Low to Medium Risk and the Medium to High Risk categories, versus having a single number dictate the change from one risk group to another. The Focus group suggested that a threshold range provides more flexibility for LDCs to choose the risk profile that best matches their unique situation, rather than defining their risk profile to a single number. They also stated that with this change the tool would be more useful for them as they judge their own risk profile.

The concept is that if the LDC's risk rating score lies within these transition ranges (also referred to as "crease points" by the Focus group members), then the LDC could choose to align to either risk profile or a combination of both. For example if an LDC's risk rating was 70, they could choose to implement all of the Low-Risk controls (at minimum), all of the Medium-Risk controls, or the Low-Risk controls with some Medium-Risk controls.

For an LDC with a risk profile rating in the transition range, it is recommended that in addition to implementing the controls from the lower risk area they should implement some or all of the highest priority controls in the higher risk area. Prioritization of controls is discussed in the proposed changes to the security controls spreadsheet, which works very well with these transition ranges.

All of the suggested changes by the Focus group were incorporated into the Inherent Risk Profile Tool, and the revised tool is provided for review with this report.

In addition to the Inherent Risk Tool, the Focus group also reviewed in detail the Security Controls spreadsheet. The following summarizes the proposed changes to the Security Controls spreadsheet from the Focus Group:

SECURITY CONTROLS SPREADSHEET SUGGESTED CHANGES FROM THE FOCUS GROUP

Control Affected	Proposed Change
RS-AN.3	Added definition of computer forensics to the illustrative examples column. Used text by Kruse, Heiser from their 2002 publication "Computer Forensics: Incident Response Essentials"
RS-AN (1,2,4), RS-MI (1,2)	Five controls added to medium risk group requirements
All	Added priorities for Low, Medium and High-Risk controls. Priority defined as #1, 2 and 3.

The Medium Risk group felt that most of the security controls needed for incident response should be required for their organizations. From AESI's perspective we would suggest one exception for inclusion: RS-AN.3 "Forensics are performed". Forensics in the true sense is a highly specialized skill set and requires a high level of technological capability that may be greater than what most Medium Risk organizations can achieve for some time. As such, this control was not added to the list of Medium Risk Controls. Should a Medium Risk entity be capable of performing forensics, then they can add this control to their control list on their own decision.

All three Focus groups wanted to have guidance on the priority for their respective security controls. All LDCs will have partially implemented their required security controls. So then the question is what controls should be addressed first? In one of the Focus group meetings, the participants discussed this in detail and then established their recommended priorities for each control in Low, Medium and High-Risk areas.

All of the suggested changes by the Focus group were incorporated into the Security Controls spreadsheet, and the revised is provided for review with this report.

2.2.2. Implementation

The Focus groups discussed and provided suggestions for the implementation of the Framework in the areas of support, tools and resources.

IMPLEMENTATION SUGGESTIONS FROM THE FOCUS GROUP

Category	Summary of Suggestions
Support	• Establish industry mentoring program • Leverage existing industry forums • Share/lend LDC resources
Vendors	• Support for LDCs in vendor discussions • Shared vendor solutions • Organize buying groups for vendor products and services
OEB	• Recommend that the OEB continue to facilitate the implementation of the Framework. The Focus group noted that without facilitation the initiative could fail. • Want all LDCs committed to the Framework with OEB support • Possibility for OEB to lead for a limited time and then hand off to long-term authority? • The long-term owner of the Framework should not also act as an auditor. • Concern that if the implementation mandate is too loose that the implementation will not be successful • Need entity defined to be available to answer long-term questions at the release of the framework
Tools	• Develop SAQ tool to provide visualization of status at any time, as it would be very useful for communicating to LDC Executive Team and Board • Develop Implementation Guide Books – Operational Level & Board Level • Additional “How To” guidance to be provided
General	• Emulate industry implementation of smart metering

3. Attaining the Initial Achievement Levels

The following are the Maturity Indicator Levels (MIL) in the DOE-C2M2 model that is referenced in the security controls spreadsheet:

Initial Achievement Level
MIL0: Not Performed
MIL1: Initiated
MIL2: Repeatable
MIL3: Managed/Adaptive

For the initial achievement levels for the three risk profiles, MIL1 was selected as the starting point. There will be a specified period of time allocated for the LDCs to attain the initial achievement levels. And then from there, as appropriate, maturity progress will be required (i.e., MIL1 to MIL2/3) over time.

Low-Risk Focus Group:

Members of Low-Risk Focus Group estimated that it would take approximately two years to transition their organizations from their current achievement level in 2017 to reach an initial MIL1 achievement level. There was an expectation that this effort would require at least 2000 man-hours or approximately one full-time equivalent resource working throughout the two years to achieve this target.

Medium Risk Focus Group:

Members of Medium Risk Focus Group estimated that transitioning their organizations from 2017 levels to an initial MIL1 achievement level would require two to four years to accomplish. There was some discussion by this group of needing to balance the cost of implementing controls against the risk each organization was willing to accept. The extent to which an organization was willing to accept a certain level of risk would have a significant impact on the length of time needed to achieve the target MIL1 level.

High Risk Focus Group:

The general consensus of High Risk Focus Group was that many had made great strides towards MIL1 level for most controls, and some were working towards MIL2 level implementation. It was recognized that work is required to align current and past efforts to the specifics of the Framework.

4. Recommendations for Industry Implementation of the Framework

The following table summarizes AESI's recommendations for the short term implementation of the Framework and longer term aspirational evolutionary initiatives. These recommendations are based on the comment period feedback from Stakeholders, the Focus group feedback, other considerations from the White Paper, and specific feedback from the CSWG meeting on November 13, 2017.

Long-Term recommendations suggest a path to increasing the overall efficacy and capability of the sector and recognizes risks attributed to the integrated nature of the grid. These include increased data collection, measurement and analysis, broader sharing, and outreach with other organizations and associations to leverage their experience and develop more universal processes. Most of these recommendations will need to be accepted by stakeholders, before proceeding.

FRAMEWORK INDUSTRY IMPLEMENTATION RECOMMENDATIONS

Area	Short Term	Long-Term
Support	• Additional tools are provided (e.g., SAQ visualization, Implementation Guide Book, industry guidance, etc.). Include examples, clarifications and implementation roadmap • Industry training be established • Co-ordinated effort for vendor support should be emphasized • Industry mentoring program be established • Leverage existing industry forums for additional support • Implementation Guidebook should be top priority to support framework – both operation and board level guides • Availability of Board Reporting Templates	• Security maturity information and analytics be provided • Industry standardized KRIs be developed
Evolution	• Finalize Inherent Risk Profile Tool and the Security Controls spreadsheet • Coordination with the gas distribution sector • Coordination with IESO and Ontario's Bulk Electric System (BES)	• Coordination first with the Canadian Cyber Threat Exchange (CCTX) and the applicable Information Sharing and Analysis Centers (ISACs); and then from there CSA, NERC, Canadian Security Establishment, and others as applicable. • Determine synergies with other industry associations (e.g., APPA, NRECA) • Coordination with NIST's Cybersecurity Framework team • Coordination with US Fusion / Threat Intelligence Centers as applicable

		• Need to prioritize this list as they may require significant personnel, time and funding commitments
Cost	• Each LDC to itemize current CAPEX and OPEX spending on cyber security • Each LDC to determine required CAPEX and OPEX budget to achieve compliance • Expectation to utilize OPEX for implementation in most cases • Find mechanism to measure effectiveness of expenditures	• Each LDC to identify cyber security CAPEX and OPEX and budget for these costs in the LDC's standard budget process • Resolve disconnect between 10 yr rate filing window and shorter cyber security life cycles • Can't itemize cyber initiatives, need a regulatory framework to accomplish
Governance	LDC: • The LDC's Executive Team and Board to be engaged and supportive of the LDC's cyber security program • Perception that current Boards already appreciate importance of cyber security • Board level guide to support implementation would be beneficial Industry: • OEB to continue to facilitate the implementation of the Framework while seeking industry facilitator • Creation of the Cyber Security Advisory Committee (CSAC) • Creation of the Cyber Security Information Sharing Forum (CSIF) • Establish time period for LDCs to achieve initial compliance levels • Develop common reporting framework for LDC's to use • Need identified authority available to answer long-term questions when framework released	LDC: • Continue to evolve and achieve higher maturity levels Industry: • Establish Framework facilitator • Finalize Centralized Compliance Authority • If IESO will eventually act as an auditor, they should not be the long-term owner of the framework

Appendix A: Glossary of Terms and Abbreviations

American Gas Association (AGA): Represents more than 200 local energy companies that deliver clean natural gas throughout the United States. (www.aga.org)

American Public Power Association (APPA): The service organisation for the more than 2,000 U.S. community-owned electric utilities that serve more than 47 million Americans. APPA was created in September 1940 to represent the common interests of these utilities. Today, APPA's purpose is to advance the public policy interests of its members and their consumers and provide member services to ensure adequate, reliable electricity at a reasonable price with the proper protection of the environment. Regular APPA membership is open to U.S. public power utilities, joint action agencies (state and regional consortia of public power utilities), rural electric cooperatives, Canadian municipal/provincial utilities, public power systems within U.S. territories and possessions, and state, regional, and local associations in the United States and Canada that have purposes similar to APPA. (www.publicpower.org)

Bulk Electric System (BES): Unless modified by the lists shown in the NERC Glossary of Terms, all Transmission Elements operated at 100 kV or higher and Real Power and Reactive Power resources connected at 100 kV or higher. This does not include facilities used in the local distribution of electric energy. See NERC Glossary of Terms[4] for a list of Inclusions and Exclusions. (NERC)

Bulk Power System (BPS): The interconnected electrical systems within northeastern North America comprised of system elements on which faults or disturbances can have a significant adverse impact outside of the local area. (NPCC)

Canadian Energy Pipeline Association (CEPA): Represents Canada's transmission pipeline companies who operate approximately 119,000 kilometres of pipeline in Canada and 15,000 kilometres in the United States. (www.cepa.com)

Control Objectives for Information and Related Technologies (COBIT): An information technology and control good practice framework created by the Information Systems Audit and Control Association (ISACA) for information technology (IT) management and IT governance.

Cyber Assets (CAs): Programmable electronic devices, including the hardware, software, and data in those devices. (NERC)

Distributed Energy Resources (DERs) are smaller power sources that can be aggregated to provide the power necessary to meet regular demand. As the electricity grid continues to

[4] Glossary of Terms.pdf

modernise, DER such as storage and advanced renewable technologies can help facilitate the transition to a smarter grid.

Distributed Network Protocol (DNP3): A set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Electricity Sector Information Sharing and Analysis Center (E-ISAC): Gathers and analyses security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the Electricity Subsector, across interdependent sectors, and with government partners. The E-ISAC, in collaboration with the Department of Energy and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the Electricity Subsector and enhances the subsector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents. The E-ISAC is operated on behalf of the Electricity Subsector by the North American Electric Reliability Corporation. (www.eisac.com)

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.

Federal Energy Regulatory Commission (FERC): An independent agency that regulates the interstate transmission of natural gas, oil, and electricity. FERC also regulates natural gas and hydropower projects. (www.ferc.gov)

Federal Financial Institutions Examination Council's (FFIEC): A formal U.S. government interagency body that includes five (5) banking regulators—the Federal Reserve Board of Governors (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). (www.ffiec.gov)

Framework: Provide guidelines without being too detailed or rigid. Frameworks give the organisation the liberty of customising the structure based on their business needs. Frameworks can be represented with diagrams with little documentation.

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.

Governance, Risk Management and Compliance (GRC): GRC is three pillars that work together for the purpose of assuring that an organisation meets its objectives. Governance is the combination of processes established and executed by the board of directors that are reflected in the organisation's structure and how it is managed and led toward achieving goals. Risk management is predicting and managing risks that could hinder the organisation to achieve its objectives. Compliance with the company's policies and procedures, laws and regulations, strong and efficient governance is considered key to an organisation's success. GRC is a discipline that aims to synchronise information and activity across governance, risk management and compliance in order to operate more efficiently, enable effective information sharing, more effectively report activities and avoid wasteful overlaps.

Independent Electricity System Operator (IESO): The IESO is a not-for-profit corporate entity established in 1998 by the Electricity Act of Ontario. It is governed by an independent Board whose Chair and Directors are appointed by the Government of Ontario. Its fees and licences to operate are set by the Ontario Energy Board and it operates independently of all other participants in the electricity market. (www.ieso.ca)

Independent System Operators (ISOs): Operates a region's electricity grid, administers the region's wholesale electricity markets, and provides reliability planning for the region's bulk electricity system.

Industrial Control Systems (ICyber Security): Encompasses several types of control systems used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCyber Security), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures.

Information Technology (IT): Refers to the corporate business systems and applications.

Intelligent Electronic Device (IED): Microprocessor-based controllers of power system equipment, such as circuit breakers, transformers and capacitor banks

Inter-Control Center Communications Protocol (ICCP): Allows the exchange of real-time and historical power system information including status and control data, measured values, scheduling data, energy accounting data and operator messages.

International Electrotechnical Commission (IEC): Prepares and publishes International Standards for all electrical, electronic and related technologies. (www.iec.ch)

International Organization for Standardization (ISO): ISO is an independent, non-governmental international organisation with a membership of 163 national standards bodies. Through its members, it brings together experts to share knowledge and develop voluntary, consensus-based, market-relevant international standards that support innovation and provide solutions to global challenges. (www.iso.org)

Internet Protocol Security (IPsec): A protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

Intrusion Detection System (IDS): A device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a SIEM system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

Intrusion Prevention System (IPS): A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. Vulnerability exploits usually come in the form of malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine.

Joint Action Agencies (JAAs): A body consisting of utility companies, municipalities who own public utilities, and/or municipalities who purchase energy from private utilities, which acts as a committee for making decisions regarding the acquisition and delivery of energy resources or related services.

Local Distribution Company (LDC): Refers to the companies that make up Ontario's electrical distribution network including small, medium and large utilities. Local distribution companies are responsible for delivering electricity, transformed from the high-voltage transmission system to the low-voltage distribution system, to more than four million Ontario homes, businesses and public institutions. Local distribution companies deal directly with residents and small businesses, create and implement conservation programs and maintain local distribution wires. There are about 80 local distribution companies in the province. They are both publicly and privately owned with the majority being owned by municipalities. Local distribution companies are regulated monopolies in their respective communities and service areas. Their rates are regulated by the Ontario Energy Board. (http://microfit.powerauthority.on.ca/local-distribution-companies)

Low Impact BES Cyber System Electronic Access Point (LEAP): A Cyber Asset interface that controls Low Impact External Routable Connectivity. The Cyber Asset containing the LEAP may reside at a location external to the asset or assets containing low impact BES Cyber Systems. (NERC)

Low Impact External Routable Connectivity (LERC): Direct user-initiated interactive access or a direct device-to-device connection to a low impact BES Cyber System(s) from a Cyber

Asset outside the asset containing those low impact BES Cyber System(s) via a bi-directional routable protocol connection. Point-to-point communications between intelligent electronic devices that use routable communication protocols for time-sensitive protection or control functions between Transmission station or substation assets containing low impact BES Cyber Systems are excluded from this definition (examples of this communication include, but are not limited to, IEC 61850 GOOSE or vendor proprietary protocols). (NERC)

Market Assessment and Compliance Division (MACD): The IESO's Market Assessment and Compliance Division (MACD) monitor the operation of Ontario's electricity market and foster compliance with the Ontario market rules and North American reliability standards. It does this through its prevention, monitoring, auditing, investigation, and enforcement activities. www.ieso.ca/sector-participants/market-oversight

Methodology: Methodology uses a repeatable approach with a defined set of rules, methods, deliverables, and processes for organisations to follow.

Multiprotocol Label Switching (MPLS): A type of data-carrying technique for high-performance telecommunications networks that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA): Requires municipal institutions to protect the privacy of an individual's personal information existing in government records. The Act creates a privacy protection scheme, which the government must follow to protect an individual's right to privacy. The scheme includes rules regarding the collection, use, disclosure and disposal of personal information in the custody and control of a municipal institution. The Act also gave individuals the right to access municipal government information, including most general records and records containing their own personal information, subject to very specific and limited exemptions

National Institute of Standards and Technology (NIST): A measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. (www.nist.gov)

National Rural Electric Cooperative Association (NRECA): Represents the interests of over 900 electric cooperatives in the United States, to various legislatures. Independent electric utilities are not-for-profit and are owned by their members. (www.electric.coop)

NERC Critical Infrastructure Protection (CIP): Mandatory Reliability Standards include CIP standards 002 through 014, which address the security of Cyber Assets essential to the reliable operation of the electric grid. (NERC)

NIST Internal or Interagency Reports (NISTIR): Describe research of a technical nature of interest to a specialised audience. The series includes interim or final reports on work performed by NIST for outside sponsors (both government and nongovernment). NISTIRs may also report results of NIST projects of transitory or limited interest, including those that will be published subsequently in more comprehensive form.

North American Electric Reliability Corporation (NERC): A not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC’s area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organisation (ERO) in North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people. NERC is the US Federal Energy Regulatory Commission (FERC) certified Electric Reliability Organization (ERO) for the United States and confirmed by Ontario Ministry of Energy on November 28, 2006, as the ERO for Ontario and as the successor to the former North American Electric Reliability Council. NERC is a "*Standards Authority*" within the meaning of the Electricity Act, 1998 (Ontario) and the Ontario Market Rules, having the purpose of enhancing the reliability of the international, interconnected bulk power systems in northeastern North America through the development of continent-wide Reliability Standards. (www.nerc.com)

Office of the Information and Privacy Commissioner of Ontario (IPC): The function of the office is to uphold and promote open government and the protection of personal privacy in Ontario, established as an officer of the Legislature by Ontario's Freedom of Information and Protection of Privacy Act (FIPPA). The IPC also has responsibility for the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA). Together, these three Acts establish rules about how the institutions covered may collect, use, and disclose personal data. They also establish a right of access that enables individuals to request their own personal information and have it corrected if necessary. (www.ipc.on.ca)

Open Web Application Security Project (OWASP): an Online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. (www.owasp.org)

OpenSSL: A software library to be used in applications that need to secure communications against eavesdropping or need to ascertain the identity of the party at the other end. It has found wide use in internet web servers, serving a majority of all websites.

Operational Technology (OT): Refers to the systems and applications that are related to grid operations.

Payment Card Industry (Data Security Standard) (PCI DSS): The PCI Security Standards is a global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security. (www.pcisecuritystandards.org)

Personal Information Protection Electronic Documents Act (PIPEDA): Governs how private sector organisations collect, use and disclose personal information in the course of commercial business. In addition, the Act contains various provisions to facilitate the use of electronic documents.

Policy: High-level management directives and is mandatory.

Privacy by Design (PbD): Developed by the then Information and Privacy Commissioner of Ontario, Canada, Dr Ann Cavoukian, back in the '90s. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organisation's default mode of operation.

Procedure: Low level and provide step-by-step process to be followed to achieve a specific task. Procedures are mandatory.

Processes: They are well-defined steps and decisions for individuals to follow in order to execute a specific task.

Public Key Infrastructure (PKI): A Public Key Infrastructure incorporates hardware as well as software components, which are in turn managed by security policies. The main components include Public Key Cryptography, a Certificate Authority (CA), a Registration Authority (RA), a Certificate Distribution System, Security Policies, and a PKI-enabled application.

Regional Transmission Operator (RTO): An entity that is independent of all generation and power marketing interests and has exclusive responsibility for grid operations, short-term reliability, and transmission service within a region.

Remote Terminal Unit (RTU): A microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.

Risk Indicator: Is a metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite.

Security Information and Event Management (SIEM): Software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

Standard: Standards are mandatory and define processes or rules to follow the specific use of technology and are often applied to hardware and software.

Supervisory Control and Data Acquisition (SCADA): A system for remote monitoring and control that operates with coded signals over communication channels (using typically one communication channel per remote station). The control system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions. It is a type of industrial control system (ICyber Security). Industrial control systems are computer-based systems that monitor and control industrial processes that exist in the physical world. SCADA systems historically distinguish themselves from other ICyber Security systems by being large-scale processes that can include multiple sites and large distances.

Technical Interconnection Requirements (TIR): The TIR provides Hydro One’s technical interconnection requirements for Distributed Generation interconnections at voltages 50kV and below.

US Department of Energy (DOE): a Cabinet-level department of the United States Government concerned with the United States' policies regarding energy and safety in handling nuclear material. Its responsibilities include the nation's nuclear weapons program, nuclear reactor production for the United States Navy, energy conservation, energy-related research, radioactive waste disposal, and domestic energy production. (www.energy.gov)

US Department of Homeland Security (DHS): is a cabinet department of the United States federal government with responsibilities in public security, roughly comparable to the interior or home ministries of other countries. Its stated missions involve antiterrorism, border security, immigration and customs, cybersecurity, and disaster prevention and management. It was created in response to the September 11 attacks. (https://www.dhs.gov/our-mission).

Virtual Private Network (VPN): a private network that extends across a public network or the internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs can provide functionality, security and/or network management benefits to the user. But they can also lead to new issues, and some VPN services, especially "free" ones, can actually violate their users' privacy by logging their usage and making it available without their consent or make money by selling the user's bandwidth to other users.