bcuc
British Columbia
Utilities Commission

Suite 410, 900 Howe Street
Vancouver, BC Canada V6Z 2N3
bcuc.com

P: 604.660.4700
TF: 1.800.663.1385
F: 604.660.1102

ORDER NUMBER
G-385-22

IN THE MATTER OF
the *Utilities Commission Act*, RSBC 1996, Chapter 473

and

British Columbia Utilities Commission
Establishment of a Two-Year Pilot of a Cybersecurity Framework for Public Utilities

BEFORE:
David Morton, Chair

on December 23, 2022

ORDER

WHEREAS:

A. The BCUC has general supervision of all public utilities pursuant to section 23 of the *Utilities Commission Act* (UCA). Further, pursuant to section 38 of the UCA, a public utility must provide and maintain its property and equipment in a condition that enables it to provide service to the public that the BCUC considers is in all respects adequate, safe, efficient, just and reasonable;

B. BCUC staff conducted a high-level cybersecurity survey in 2022, the results of which indicate a wide variance in the ability of public utilities to mitigate cybersecurity risk;

C. The BCUC has observed increasing rates and severity of cyber-attacks globally and within Canada and the significant costs to recover from cybersecurity incidents;

D. The BCUC has developed a framework to address cybersecurity risk for public utilities (Cybersecurity Framework). The Cybersecurity Framework is flexible and scalable based on size and risk of the public utility and makes use of existing industry guidance for regulatory efficiency;

E. The BCUC proposes to introduce the Cybersecurity Framework on a two-year pilot basis to assess its effectiveness in addressing public utility cybersecurity risk (Pilot). At the completion of the Pilot, the BCUC will consider adopting the Cybersecurity Framework on a permanent basis; and

F. The BCUC considers that a public utility comment process to consider the establishment of the Pilot is warranted.

NOW THEREFORE the BCUC orders as follows:

1. A regulatory timetable is established, as set out in Appendix A to this order.

2. Public utilities are invited to submit letters of comment for the BCUC's consideration on the following:

   i) The establishment of the Pilot;

   ii) The Cybersecurity Framework for Public Utilities attached as Appendix B1 to this order; and

   iii) The Annual Cybersecurity Declaration for Public Utilities attached as Appendix B2 to this order.

3. Letters of comment must be submitted by the date established in the regulatory timetable attached as Appendix A to this order in the Letter of Comment Form and be submitted on the BCUC's website, or submitted by email to commission.secretary@bcuc.com, mail, courier or personal delivery to the British Columbia Utilities Commission, Suite 410, 900 Howe Street, Vancouver, BC V6Z 2N3.

DATED at the City of Vancouver, in the Province of British Columbia, this 23rd day of December 2022.

BY ORDER

Original signed by:

D. M. Morton
Commissioner

Attachment

British Columbia Utilities Commission
Establishment of a Two-year Pilot of a Cybersecurity Framework for Public Utilities

REGULATORY TIMETABLE

Action	Date (2023)
Letters of comment from Public Utilities	Thursday, March 2
Further process	To be determined

bcuc
British Columbia
Utilities Commission

Suite 410, 900 Howe Street
Vancouver, BC Canada V6Z 2N3
P: 604.660.4700
TF: 1.800.663.1385
F: 604.660.1102

Cybersecurity Framework for Public Utilities

Version 1.0

1.0 BACKGROUND

The British Columbia Utilities Commission (BCUC) has general supervision of all public utilities pursuant to section 23 of the *Utilities Commission Act* (UCA). Further, pursuant to section 38 of the UCA, a public utility must provide and maintain its property and equipment in a condition that enables it to provide service to the public that the BCUC considers is "in all respects adequate, safe, efficient, just and reasonable". The BCUC expects public utilities to mitigate cybersecurity risks to their systems to ensure safe and reliable service.

The BCUC surveyed commonly adopted cybersecurity standards and frameworks and, based on its assessment, considers the National Institute of Science and Technology (NIST) Cybersecurity Framework version 1.1 to be the most suitable for adoption in British Columbia (BC). In the sections below, the BCUC sets out its expectations for how public utilities will implement the NIST Framework.

2.0 TERMS AND DEFINITIONS

The following terms and definitions are used:

Term	Definition
Associated Cyber Asset	A cyber asset that is on the same physical or logical network segment as a Critical Cyber Asset and is not considered a Critical Cyber Asset. An Associated Cyber Asset must be protected in the same manner as a Critical Cyber Asset.
Applicable Systems	Critical Cyber Systems owned or operated by a public utility in BC that are necessary for the safe and adequate delivery of Service. Applicable Systems exclude BES Cyber Systems.
BES Cyber System	BES Cyber Systems as defined in the NERC Glossary of Terms,[1] are subject to compliance with the MRS in BC. BES Cyber Systems are excluded from Applicable Systems.
BES	Bulk Electric System as defined in the NERC Glossary of Terms.
Critical Cyber Asset	A cyber asset that, if its availability, integrity or confidentiality were compromised, could adversely impact the Service of the public utility.
Critical Cyber System	A cyber system comprising Critical Cyber Assets, that is used to manage one or more functions associated with the public utility's Service. A Critical Cyber System includes Associated Cyber Assets on the same physical or logical network segment as Critical Cyber Assets.
IT	Information Technology, includes computers, network devices, security devices and other equipment used for business processes such as customer management, billing, accounting, etc.
MRS	Mandatory Reliability Standards adopted by the BCUC.
NERC	North American Electric Reliability Corporation.
NIST	National Institute of Science and Technology.
OT	Operational Technology, includes computers, network devices, process controllers, remote terminal units, measurement devices, sensors and other equipment used to monitor and

[1] https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Term	Definition
	control operational processes such as power generation and distribution, steam generation and distribution and gas distribution.
Service	As defined in the UCA, Service includes (a) the use and accommodation provided by a public utility, (b) a product or commodity provided by a public utility, and (c) the plant, equipment, apparatus, appliances, property and facilities employed by or in connection with a public utility in providing service or a product or commodity for the purposes in which the public utility is engaged and for the use and accommodation of the public.

3.0 APPLICABILITY

The BCUC expects public utilities actively regulated by the BCUC to implement a cybersecurity program based on the NIST Cybersecurity Framework for their Applicable Systems. Public utility BES Cyber Systems subject to MRS compliance are excluded. Applicable Systems include Information Technology (IT) Critical Cyber Systems and Operational Technology (OT) Critical Cyber Systems necessary to provide safe and adequate Service.

4.0 NIST CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework Overview

The NIST Cybersecurity Framework includes three key components: (i) the Framework Core; (ii) Framework Implementation Tiers; and (iii) Framework Profiles.

The Framework Core provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand. The Framework Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

The Framework Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management. The Implementation Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Framework Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

BC Implementation Approach

Public utilities that have only a basic cybersecurity program are expected to improve that program or establish a new cybersecurity program based on the NIST Cybersecurity Framework. Public utilities that already have a well-established cybersecurity program based on other standards or frameworks may instead map that program to the NIST Cybersecurity Framework for their Applicable Systems.

If a public utility does not implement the NIST Cybersecurity Framework, or if the BCUC has concerns with the adequacy of the program, the BCUC may investigate the adequacy of a public utility's cybersecurity risk mitigation preparedness. If the BCUC finds, upon holding a hearing, that the public utility has not implemented adequate cybersecurity measures, such that the Service provided by that utility is not in all respects safe and adequate then the BCUC may order the utility to implement specific cybersecurity measures.

Establishing a Cybersecurity Program

The BCUC expects public utilities to review and follow the seven-step process documented by the NIST Cybersecurity Framework to establish and/or improve their cybersecurity program. The steps are:

1. Prioritize and scope
2. Orient
3. Create a current Profile
4. Conduct a risk assessment
5. Create a target Profile
6. Determine, analyze and prioritize gaps
7. Implement action plan

Please refer to the NIST Cybersecurity Framework version 1.1[2] for more information on the development and improvement of a cybersecurity program. The BCUC may issue implementation guidance from time to time.

The BCUC expects public utilities to report to the BCUC all cybersecurity incidents that impact a Critical Cyber System, within two business days of the detection of the incident and provide periodic updates until the incident is declared closed.

Review and Reporting

The BCUC expects that each public utility will inform the BCUC via email to commission.secretary@bcuc.com when it has implemented its cybersecurity program based on the NIST Cybersecurity Framework. The BCUC further expects that each public utility will review their cybersecurity program annually, identify gaps and opportunities for improvement and create a corrective and improvement actions plan. The public utility will also submit an annual declaration to the BCUC in the format shown as Attachment B-2. The BCUC may conduct a detailed review of the cybersecurity program if warranted.

Data Storage, Retention and Security

The BCUC recommends that public utilities hold all information and records pertaining to cybersecurity securely to ensure they are adequality protected. Cybersecurity program review records, evidence of conformance with the cybersecurity controls and other records be retained for a minimum of five years. The BCUC also recommends that all cybersecurity information stored outside the public utility's premises and digital infrastructure reside within Canada, whether in physical or in electronic form.

[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Confidentiality

The confidentiality of all cybersecurity information collected by the BCUC will be determined in accordance with the BCUC's Rules of Practice and Procedure.

bcuc
British Columbia
Utilities Commission

Suite 410, 900 Howe Street
Vancouver, BC Canada V6Z 2N3
bcuc.com

P: 604.660.4700
TF: 1.800.663.1385
F: 604.660.1102

Annual Cybersecurity Declaration for Public Utilities

Filing Instructions		
This declaration is to be completed annually by the public utility, as defined in section 1 of the *Utilities Commission Act* (UCA). The completed declaration is to be signed by an authorized officer of the public utility and submitted to the Commission Secretary at commission.secretary@bcuc.com. If email is unavailable, please mail the form to the address above.		
Applicant Information		
Public Utility Name:	BC Business Registration No.:	
Contact Address:		
Contact Phone:	Contact Email:	
Declaration reporting period:	*This annual declaration is due no later than 2 months after the fiscal year end*	
Cybersecurity Declaration		
Cybersecurity Function	**Implemented**	**Explanation for "No" or "Partial"**
1. A Senior Manager in the public utility is responsible for cybersecurity.	Yes No ◯ ◯	
2. A cybersecurity program has been established and is reviewed annually by the designated Senior Manager.	Yes No ◯ ◯	
3. Cybersecurity roles are established and communicated to employees and external partners. The public utility has a training and awareness program to help personnel understand cybersecurity risks.	Yes No Partial ◯ ◯ ◯	
4. Asset and configuration changes to Critical Cyber Systems are made through a configuration and change management process.	Yes No Partial ◯ ◯ ◯	
5. Security updates are applied in a timely manner to all Critical Cyber System assets.	Yes No Partial ◯ ◯ ◯	
6. The public utility has a contingency management plan for Critical Cyber Systems backups, restoration and cybersecurity incident response.	Yes No Partial ◯ ◯ ◯	
7. The public utility has contracts with third-party service providers that include cybersecurity terms and conditions.	Yes No Partial ◯ ◯ ◯	

Form: ADCSF-2022

Annual Cybersecurity Declaration for Public Utilities

8. Physical and electronic access to Critical Cyber Systems hardware and software is restricted to authorized personnel. Permissions are periodically reviewed. Strong password policies are implemented.	Yes ○ No ○ Partial ○	
9. Malware detection and protection tools are installed on Critical Cyber Systems assets.	Yes ○ No ○ Partial ○	
10. Only authorized USB drives and other removable media are permitted to be used with Critical Cyber Systems.	Yes ○ No ○ Partial ○	
11. The public utility has notified BCUC of all cybersecurity incidents that impacted Critical Cyber Systems.	Yes ○ No ○	

I am authorized to make this declaration on behalf of the public utility and have sufficient access to the public utility's records to accurately complete this declaration. The information set out herein is complete and accurate, to the best of my knowledge, information, and belief. I have read and understand the *Utilities Commission Act*.

Signature of Authorized Signing Officer

Name:

Official Title:

Date:

Instructions to fill the form

1. Please respond to all the items in the declaration.
2. Please include a brief explanation for responses that are "No" or "Partial.
3. This is not a comprehensive list of functions that a public utility may implement. Please attach brief descriptions of other cybersecurity functions that a public utility may have implemented.
4. Please attach confidential information in a separate document, if required, clearly marked as confidential. The confidentiality of all cybersecurity information collected by the BCUC will be determined in accordance with the BCUC's Rules of Practice and Procedure.
5. Please refer to APPENDIX B1 for definitions of terms.

Form: ADCSF-2022

bcuc
British Columbia
Utilities Commission

Suite 410, 900 Howe Street
Vancouver, BC Canada V6Z 2N3
P: 604.660.4700
TF: 1.800.663.1385
F: 604.660.1102

British Columbia Utilities Commission

Cybersecurity Technical Report
December 2022

Table of Contents

EXECUTIVE SUMMARY

The British Columbia Utilities Commission (BCUC) is an independent regulatory agency of the British Columbia (BC) government, operating under and administering the *Utilities Commission Act* (UCA). The BCUC is responsible for ensuring safe and reliable energy supply at fair rates for energy users across the province. The BCUC balances this responsibility with the need to ensure public utilities under its jurisdiction are afforded a reasonable opportunity to earn a fair return on their investments.

The BCUC has general supervision of all public utilities pursuant to section 23 of the UCA. Further, pursuant to section 38 of the UCA, public utilities must provide and maintain their property and equipment in a condition that enables them to provide service to the public that the BCUC considers is "in all respects adequate, safe, efficient, just and reasonable". The BCUC also adopts and enforces the Mandatory Reliability Standards (MRS) developed by the North American Electric Reliability Corporation and approved by the United States Federal Energy Regulatory Commission. The MRS are applicable to all entities that have facilities associated with the Bulk Electric System (BES) in BC (MRS Registrants). Entities include public utilities for Facilities that are associated with the BES and thus in scope for compliance with the MRS.

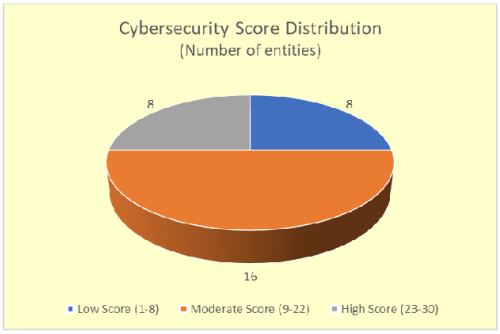
The BCUC considers cyber risk to be a significant threat to the province's public utilities and MRS Registrants (together, Regulated Entities). Cybercrime has been increasing steadily over the years and 2021 saw a significant increase in cyber-attacks during the COVID-19 pandemic. Canadian organizations and individuals were amongst those targeted in these attacks. The BCUC sent "INFORMATION BULLETIN 21-01 – Regulated Entities and Cybersecurity" (Attachment 1) on February 8, 2021, to Regulated Entities, informing them that cyber risk is a significant threat to safe and reliable energy supply in BC. The BCUC also stated that Regulated Entities are expected to mitigate cyber risk exposure and establish a plan to respond effectively in the event of a cyber-attack.

As a follow up to the Information Bulletin from 2021, the BCUC sent a letter and brief survey requesting information about the measures Regulated Entities had implemented to mitigate cybersecurity risks. The intent of the survey was to develop a high-level understanding of Regulated Entities' capability to mitigate cybersecurity risks. Cybersecurity scores were assigned to Regulated Entity responses. The maximum score is 30.

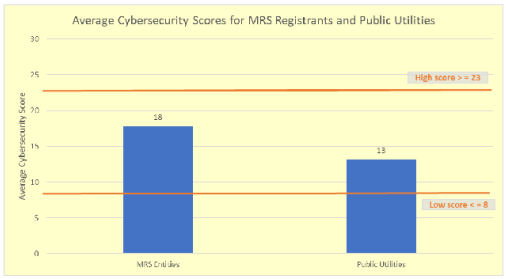
Findings from the survey

The BCUC's key findings from the survey are:

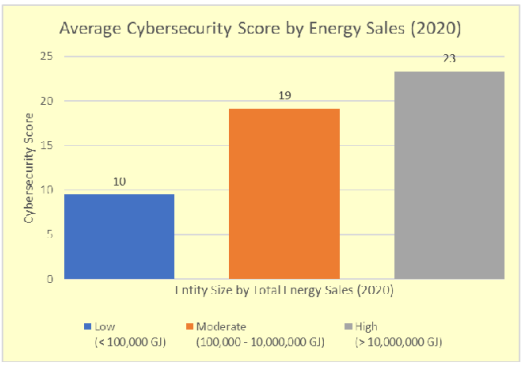
- Of the 32 responses, eight scored Low (1 – 8), 16 responses scored Moderate (9 – 22) and the remaining 8 scored High (23 – 30).



- Cybersecurity scores were generally higher for MRS Registrants than for public utilities.[1] MRS Registrants must comply with mandatory cybersecurity standards for applicable cyber assets.



- Cybersecurity scores appear to have a correlation with the size of the Regulated Entity – entities with higher energy sales obtained higher cybersecurity scores on their survey responses, as did entities with higher revenues or a larger number of customers.



[1] For the purposes of this report, survey scores for Regulated Entities that are both public utilities and MRS Registrants were included in both categories.

Approaches to mitigate cyber risk

MRS Registrants must comply with mandatory Critical Infrastructure Protection (CIP) standards. Their responses received higher cybersecurity scores than public utility responses, where similar mandatory cybersecurity standards are not in place today. A successful cyber-attack may adversely impact a public utility's critical systems, resulting in disruption of energy supply or services to the public. Confidential customer information that is expected to be safeguarded by the public utility is at risk of being stolen and potentially misused for fraudulent purposes.

The BCUC considers cybersecurity essential for a public utility to maintain safe and adequate service to the public and expects that public utilities will implement a cybersecurity program for critical infrastructure that is out of the scope of MRS (Applicable Systems). Public utilities are responsible for the cybersecurity of their systems and information hosted by or outsourced to third parties. The BCUC also has an obligation under section 24 of the UCA to keep itself informed about the conduct of the province's public utilities in this respect.

The BCUC assessed the following alternatives to mitigate cybersecurity risks for public utilities for their Applicable Systems:

Alternative	Brief Description
Maintain status quo	Public utilities implement cybersecurity risk mitigation measures for their Applicable Systems as they deem appropriate, and no further action is required by the BCUC.
Adopt an existing cybersecurity framework	Adopt the National Institute of Science and Technology (NIST) Cybersecurity Framework for public utility Applicable Systems.
Develop custom cybersecurity framework	Develop a new cybersecurity framework specifically for public utility Applicable Systems.

Survey findings indicate that 25% of Regulated Entities have a low level of cybersecurity risk mitigation capability and that 50% have only a moderate capability; thus putting these groups at a higher risk of a successful cyber-attack. The implication is that maintaining status quo may continue to increase risk to public utilities that have a basic program for their Applicable Systems.

The NIST Cybersecurity Framework is a customizable and extensible framework that has been widely adopted across sectors, including for public utilities. This framework appears to be well-suited for adoption in BC for public utility Applicable Systems.

There are several well-known and widely adopted cybersecurity standards and frameworks. Creating a new cybersecurity framework from the ground up would be resource and time intensive.

As such, the BCUC considers adoption of the NIST Cybersecurity Framework to be the most appropriate approach for BC.

1.0 INTRODUCTION

The British Columbia Utilities Commission (BCUC) is an independent regulatory agency of the British Columbia (BC) government, operating under and administering the *Utilities Commission Act* (UCA). The BCUC is responsible for ensuring that BC's public utilities provide safe and reliable service at just and reasonable rates. The BCUC is also responsible for the adoption and enforcement of BC's Mandatory Reliability Standards (MRS).

In the UCA, a "public utility" is defined as a person, or the person's lessee, trustee, receiver or liquidator, who owns or operates in BC, equipment or facilities for the production, generation, storage, transmission, sale, delivery or provision of electricity, natural gas, steam or any other agent for the production of light, heat, cold or power to or for the public or a corporation for compensation. There are a number of exclusions from the definition of a public utility, including municipalities or regional districts that provide services within their own boundaries, and a person that provides services to employees or tenants.

A "service" is defined in the UCA as including (a) the use and accommodation provided by a public utility, (b) a product or commodity provided by a public utility, and (c) the plant, equipment, apparatus, appliances, property and facilities employed by or in connection with a public utility in providing service or a product or commodity for the purposes in which the public utility is engaged and for the use and accommodation of the public.

Entities in BC that own and/or operate Bulk Electric System (BES)[2] Facilities[3] that are part of the North American Bulk Electric System are required to comply with the MRS. BES Facilities typically include power generation systems over a certain threshold, high voltage transmission systems (over 100 kV) and Control Centers; thus, most local low voltage distribution systems owned or operated by public utilities are out of scope of the MRS.

Entities that are required to comply with the MRS include:

- Independent Power Producers that generate electricity for sale;
- public utilities that own and/or operate BES Facilities;
- industrial electricity consumers that have interconnections that qualify as BES Facilities; and
- other entities that own and/or operate BES Facilities.

Pursuant to section 125.2 of the UCA, the BCUC must review reliability standards developed by NERC, the Western Electricity Coordination Council (WECC) or another prescribed standard-making body and determine whether the standards are in the public interest and should be adopted in BC. All standards adopted under section 125.2 of the UCA are collectively called the MRS.[4] All entities subject to the MRS are required to register with WECC and are referred to as MRS Registrants.

[2] The BES is defined by the North American Electric Reliability Corporation (NERC) in the NERC Glossary of Terms. The Glossary was adopted by the BCUC when the MRS were initially adopted and subsequent revisions have been adopted over the years through orders associated with the annual MRS Assessment Reports.
[3] A Facility is defined in the NERC Glossary of Terms as "[a] set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)"
[4] https://www.bcuc.com/WhatWeDo/MRS

Cybersecurity is specifically addressed in the MRS through the NERC Critical Infrastructure Protection (CIP) standards, which are listed in Appendix A hereto.

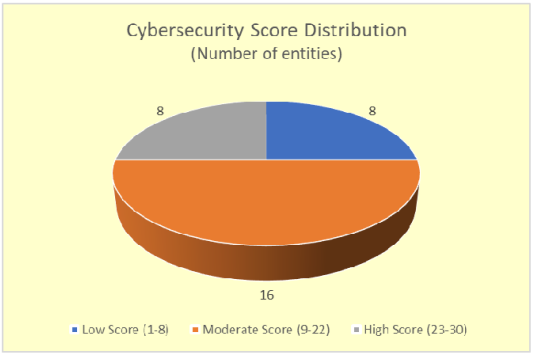
The BCUC considers cyber risk a significant threat to the province's public utilities and MRS Registrants (together, Regulated Entities). While cybercrime has become increasingly prevalent in recent years, there was a significant rise in cyber-attacks during the global COVID-19 pandemic. On February 8, 2021, the BCUC issued a bulletin[5] to Regulated Entities providing information on the significant threat cyber risk poses and indicating that Regulated Entities are expected to mitigate cyber exposure and establish a plan to respond effectively in the event of a cyber-attack.

As a follow-up to the February bulletin, the BCUC issued a letter and brief survey to Regulated Entities[6] on January 13, 2022. In the letter, the BCUC requested information about the measures Regulated Entities had implemented to mitigate cybersecurity risks. The objectives of this survey were to enable the BCUC to:

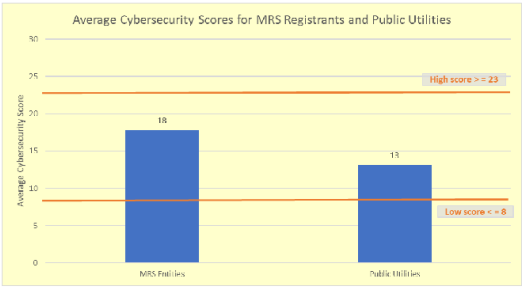
1. develop a high-level understanding of Regulated Entities' capability to mitigate cybersecurity risks; and
2. identify alternatives for further actions related to cybersecurity for Regulated Entities in BC.

The BCUC's key findings from the survey are:

- A total of 32 survey responses were assessed. Eight survey responses scored Low (1 – 8), 16 responses scored Moderate (9 – 22) and the remaining 8 scored High (23 – 30).

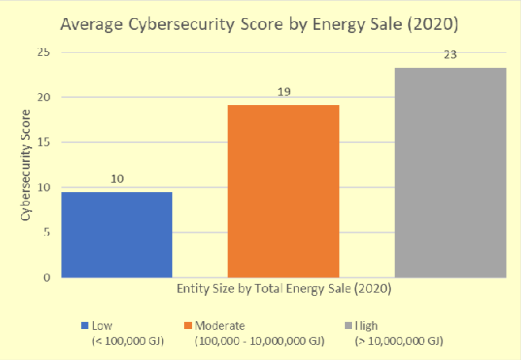


- Cybersecurity scores for MRS Registrants were generally higher than for public utilities.[7] The MRS Program requires compliance with mandatory cybersecurity standards for applicable cyber assets.



[5] INFORMATION BULLETIN 21-01 – Regulated Entities and Cybersecurity, included as Attachment 1.
[6] Stream A Thermal Energy System owners were excluded from this survey.
[7] For the purposes of this report, survey scores for Regulated Entities that are both public utilities and MRS Registrants were included in both categories.

- Cybersecurity scores appear to have a correlation with the size of the Regulated Entity – entities with higher energy sales obtained higher cybersecurity scores on their survey responses, as did entities with higher revenues or a larger number of customers.



The results of this survey show that MRS Registrants, who are required to comply with the MRS Critical Infrastructure Protection standards, generally reported higher levels of cybersecurity preparedness than public utilities that were not required to comply with any mandatory cybersecurity standards.

Section **2.0 Cybersecurity Risks and Mitigation** provides an overview of cybersecurity threats to the energy and utilities critical infrastructure. Section **3.0 BCUC Jurisdiction** discusses the BCUC's jurisdiction over the regulation of cybersecurity for public utilities**.** Finally, section **4.0 Alternative approaches** addresses alternative approaches to implement cybersecurity measures for public utility critical infrastructure that is not covered by the MRS (Applicable Systems).

2.0 CYBERSECURITY RISKS AND MITIGATION

Public Safety Canada defines critical infrastructure as "…processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government".[8] The ten critical infrastructure sectors in Canada are:

- Energy and utilities
- Finance
- Food
- Transportation
- Government
- Information and communication technology
- Health
- Water
- Safety
- Manufacturing

Public utilities and the electricity system infrastructure owned and/or operated by MRS Registrants are included in the energy and utilities critical infrastructure sector, as per the definition by Public Safety Canada. Cybersecurity threats to this critical infrastructure are constantly evolving and the consequences of cyber-attacks are increasingly disruptive, destructive and costly.

[8] https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx

Threat sources

Cybersecurity threats emerge from multiple sources, from disgruntled individuals to well-funded criminal and terrorist groups.

Threat Sources	Description	Potential Impact
Nation states	• Adversarial countries that engage in cyber warfare in addition to or as a proxy for physical war. • Have significant financial and technical resources and develop sophisticated attack tools. • Goals are to infiltrate critical infrastructure, governments and other organizations. • Disrupt economic, social and government functions. • Key drivers are geopolitical or ideological motivation.	• Theft of sensitive information. • Physical damage to critical infrastructure. • Disruption to normal functions of critical infrastructure. • Hazards to human health and safety and the environment. • Widespread social and economic adverse impact.
Criminal organizations	• Well-organized and well-funded groups that engage in criminal activities with a profit motive. • May develop their own malware, tools and techniques to infiltrate organizations. • Engage in ransomware attacks and theft of financial and personal information.	• Encryption of entire systems that are held to ransom. • Threats to publicly leak sensitive information if a ransom is not paid. • Sale of intellectual property to competitors or foreign countries. • Financial fraud through the misuse of stolen personal and financial information like social insurance numbers and credit cards.
Hacktivists	• "Hacker activists" that launch attacks on organizations that are perceived to be opposed to or in conflict with activist goals. • Attacks are often for publicity to draw attention to their cause or discredit their target organizations.	• Defacement of public web sites. • Loss of public confidence. • Loss of reputation.
Employees and contractors	• Also known as insider threats. • May be disgruntled current or former employees and contractors that look for opportunities to "get back" at the organization. • May also be current employees or contractors that have been compromised by criminal organizations with the prospect of financial gain.	• Theft of confidential information like user accounts and passwords. • Infiltration of malware. • Implanting backdoors or timebombs in enterprise software.

Threat Sources	Description	Potential Impact
Vendors and software suppliers	• Also known as supply chain attacks. • Hackers compromise software developers and IT service providers. • Use third parties and their products to insert malware into and take control of systems in their target organizations. • May target cloud service providers as a means to get to organizations whose systems are hosted on cloud platforms.	• Malware infiltration into the organization. • Unauthorized remote access to critical systems. • Deliberate malfunction or disruption of critical infrastructure. • Theft of confidential information.

Most successful attacks result in a disruption to the normal function of the target organization resulting in a loss of product and services to customers, loss of reputation and financial losses. Disruptions may also impact dependent functions such as emergency services, government and businesses.

Colonial Pipeline

A notable example of a recent cyber-attack on critical infrastructure is the attack on Colonial Pipeline in the United States in May 2021. Attackers infiltrated the Colonial Pipeline IT network and stole over 100 gigabytes of data before encrypting IT systems with ransomware. Colonial shut down their pipeline control network "out of an abundance of caution" to prevent infiltration of the ransomware into their Operational Technology (OT) network. This caused an outage of their pipeline and led to significant disruptions to the availability of gasoline and other fuels across a large portion of the eastern United States for approximately one week. Colonial Pipeline is believed to have paid $4.4 million as ransom, of which around $2.3 million was subsequently recovered from the criminals. The cause of the infiltration was stated to be an exposed password to a Virtual Private Network (VPN) account.[9]

Ukraine power grid

Another example of an attack on critical infrastructure is the disruption of part of the Ukraine power grid in December 2015. The attackers infiltrated three local electric distribution companies and took control of the Supervisory Control and Data Acquisition (SCADA) systems used to monitor and control remote substations. The attackers then manually operated breakers at 30 substations, switching off the power for approximately 230,000 customers, from one to six hours. The attackers also wiped out critical Operational Technology (OT) systems, disabled Uninterruptible Power Supplies (UPS) and corrupted the firmware of Remote Terminal Units (RTUs) to delay restoration efforts.[10]

[9] https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
[10] https://en.wikipedia.org/wiki/Ukraine_power_grid_hack

3.0 BCUC JURISDICTION

The UCA is the statute that empowers the BCUC to regulate BC's public utilities. Sections of the UCA relevant to the BCUC's role in cybersecurity for public utilities include the following.

Section 23 of the UCA grants the BCUC general supervisory responsibility for all public utilities and empowers the BCUC to issue orders over a broad range of topics, including equipment (section 23(a)) and any other matters that the BCUC considers necessary or advisable for ensuring the safety, convenience, or service of the public (section 23 (g)(i)). Further, section 23(2) authorizes the BCUC to make regulations requiring a public utility to conduct its operations in a manner that does not unnecessarily interfere with, or cause unnecessary damage or inconvenience to, the public. Given the significant and highly disruptive impact cyber-attacks can have on public utility operations, adequate cybersecurity preparedness is essential for ensuring the reliability of public utility systems. As such, the BCUC considers oversight of cybersecurity to be a necessary component of the BCUC's general supervisory responsibility.

Section 24 requires the BCUC, in executing its supervisory role, to make examinations and conduct inquiries necessary to keep itself informed about: (i) the conduct of the utility's business; (ii) the utility's compliance with the UCA and other laws and regulations; and (iii) any other matter in the BCUC's jurisdiction. While much of the language in the UCA is permissive, section 24 provides an imperative to the BCUC to remain informed about the activities of the utilities it regulates, including cybersecurity.

Section 38 of the UCA speaks to the service standard public utilities are to be held to by the BCUC as regulated entities. Pursuant to section 38, a public utility must provide and maintain its property and equipment in a condition that enables it to provide service to the public that the BCUC considers is "in all respects adequate, safe, efficient, just and reasonable". Because cyber risks pose a significant threat to the reliability of public utility systems, providing and maintaining property and equipment in a condition to enable it to provide a service to the public that the BCUC considers safe, adequate, efficient, just and reasonable includes implementation of effective cybersecurity measures.

Section 25 provides that if, after holding a hearing on its own motion or as the result of a complaint, the BCUC finds that the service of a public utility is unreasonable, unsafe, inadequate or unreasonably discriminatory, then the BCUC must take action to address the inadequacies. This includes determining what constitutes safe and adequate service and ordering the public utility to provide it.

Section 26 of the UCA provides the BCUC the authority, after a hearing held on its own motion or on complaint, to set just and reasonable standards, classifications, rules, practices or service to be used by a public utility. While section 26 does not grant the BCUC the authority to develop mandatory cybersecurity standards or rules that would be applicable to *all* public utilities, the BCUC could establish a set of recommended best practices or a cybersecurity framework that public utilities would be encouraged to adopt pursuant to the BCUC's general supervisory power under section 23 of the Act.

4.0 ALTERNATIVE APPROACHES

Cybersecurity threats have evolved rapidly with increased Internet connectivity and dependence on technology. Threat impacts have grown in magnitude and severity, from minor system crashes to entire networks being wiped out, critical business processes being held to ransom, identities being stolen for malicious use and terrorist actions that impact large segments of the population. The costs to prevent and recover from cybersecurity incidents also keep growing. Cybersecurity is no longer a "good to have" feature or intended only for large corporate entities, but rather is essential for all entities to safeguard their businesses and the private and confidential information they hold.

The BCUC has observed with growing concern the increasing frequency, sophistication and magnitude of cyber-attacks in general and on the energy sector in particular. While mandatory CIP standards are enforceable for MRS Registrants, no such standards are in place for public utilities for Applicable Systems. The BCUC has considered the following alternatives for its regulation of cybersecurity for public utility Applicable Systems. Public utilities are responsible for the cybersecurity of their systems and information hosted by or outsourced to third parties.

- Maintain the status quo;
- Adopt an existing cybersecurity standard or framework; and
- Develop a custom cybersecurity framework for BC.

Each of these alternatives is discussed below.

4.1 Maintain status quo

This alternative assumes that public utilities implement cybersecurity risk mitigation measures for their Applicable Systems as they deem appropriate, and no further action is required by the BCUC.

Findings from the high-level cybersecurity survey conducted in early 2022 indicate that there is significant variation in cybersecurity capability across the surveyed Regulated Entities. The BCUC is concerned that not all public utilities may have appropriate measures in place to mitigate cybersecurity risks, and that cyber-attacks may adversely impact the safety and adequacy of the public utility's service.

4.2 Adopt an existing cybersecurity framework

The BCUC surveyed several commonly adopted cybersecurity standards, frameworks and guidelines, and identified the National Institute of Science and Technology (NIST) Cybersecurity Framework (Framework) as a candidate for adoption in BC. The Framework was developed with the intent that it would be a voluntary baseline framework to reduce cyber risk to critical infrastructure. The Framework has been widely adopted across small and medium businesses, Federal and State government departments, academia and critical infrastructure.

NIST Cybersecurity Framework overview

The NIST Cybersecurity Framework includes three key components: (i) the Framework Core; (ii) Framework Implementation Tiers; and (iii) Framework Profiles.

The Framework Core provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand. The Framework Core guides organizations in managing and

reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

The Framework Implementation Tiers assist organizations by providing context on how an organization views cybersecurity risk management. The Implementation Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.

Framework Profiles are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Framework Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

NIST Cybersecurity Framework for public utilities

Public utility boards and other organizations that have adopted or recommended the NIST Cybersecurity Framework for regulated utilities include:

- The Ontario Energy Board has developed the Ontario Cybersecurity and Privacy Framework based on the NIST Cybersecurity Framework.
- The Connecticut Public Utilities Regulatory Authority has listed the NIST Cybersecurity Framework as one of six industry-recognized frameworks for implementation by businesses.
- The National Association of Regulatory Utility Commissioners (NARUC) recommends the NIST Cybersecurity Framework for public utility commissions to assess the cybersecurity preparedness of their regulated public utilities.

BC Implementation approach

The BCUC views the NIST Cybersecurity Framework to be a comprehensive set of safeguards whose uniform adoption could be used to ensure appropriate regulatory oversight of cybersecurity for public utility Applicable Systems. The Framework is customizable and extensible for entities of all sizes and business requirements.

Were this alternative to be adopted, the BCUC would expect all public utilities to implement the NIST Cybersecurity Framework to mitigate cybersecurity risks for their Applicable Systems and to report annually on their cybersecurity program. As necessary, the BCUC may request further individual meetings with public utilities to conduct detailed reviews of their cybersecurity programs.

If a public utility were to not implement the NIST Cybersecurity Framework, or if the BCUC had concerns with the adequacy of program delivery, the BCUC could hold a hearing to investigate the adequacy of a public utility's cybersecurity risk mitigation preparedness. If the BCUC were to find that the public utility has not implemented adequate cybersecurity measures, such that the services provided by that utility are not in all respects safe and adequate then the BCUC may order the utility to implement specific cybersecurity measures.

Establishing a cybersecurity program

The BCUC recommends that entities follow the seven-step process documented by NIST Cybersecurity Framework to establish or improve a cybersecurity program. The steps are:

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze and Prioritize Gaps
7. Implement Action Plan

Refer to the NIST Cybersecurity Framework version 1.1 [11] for more information on the process.

Review and reporting

The BCUC expects that each public utility will inform the BCUC when it has implemented its cybersecurity program based on the NIST Cybersecurity Framework. The BCUC further expects that each public utility that implements the cybersecurity program for their Applicable Systems will annually review its cybersecurity program, identify gaps and opportunities for improvement and create a corrective and improvement actions plan. The public utility will also be expected to submit an annual declaration to the BCUC in the prescribed format. The BCUC may review the cybersecurity program at its discretion.

Refer to Appendix B for more information on the NIST Cybersecurity Framework.

4.3 Develop Custom Cybersecurity Framework

An alternative to the adoption of the existing NIST Cybersecurity Framework is establishing a comprehensive cybersecurity framework specific to BC, which would be developed from the ground up. Elements to be developed would include:

- Framework governance
- Cybersecurity program definition
- Technical cybersecurity controls
- Implementation guidance
- Verification procedures

The BCUC views this as the most resource and time-intensive alternative and would require substantial investment to develop the framework and to sustain it.

Framework governance

Framework governance comprises the organization, policies, procedures and authority to conduct ongoing administration of the cybersecurity framework. This includes outreach to public utilities, development of and revisions to cybersecurity standards and processes, monitoring and other related activities.

[11] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Cybersecurity program definition

A cybersecurity program would need to be defined specifically by BC's public utilities for their Applicable Systems. The program would include requirements for cybersecurity policies and procedures, program governance, cybersecurity controls, cybersecurity risk management, cybersecurity incident management, supply chain risk management, internal and external review and verification and cybersecurity information sharing and reporting.

Cybersecurity controls

A cybersecurity standard would need to be developed for BC. The standard would identify the technical and administrative security controls that must be implemented to mitigate cybersecurity risks. The controls would address program governance, risk management, asset management, device configuration management, network management, personnel risk assessments, incident management, backup and recovery, vulnerability management, user access controls, physical security controls, security event monitoring and verification of security controls.

Tools would also be required to customize the cybersecurity program to be appropriate for the various public utilities, since this is not a one size fits all solution. Smaller public utilities or public utilities with a lower risk exposure may have a smaller set of controls than larger public utilities or those with higher risk exposures.

Implementation guidance

Implementation guidance would need to be developed to provide background information and technical guidance on the implementation of the requirements of a custom cybersecurity program. Implementation guidance may include different scenarios and suggested methods on how to implement security controls for those scenarios.

Verification procedures

Verification procedures would also be developed to verify conformance with the requirements of the cybersecurity framework. There may be multiple methods for verification, including internal reviews, external audits, third-party certification and periodic reports.

The BCUC may request further individual meetings with public utilities to conduct detailed reviews of their cybersecurity programs.

5.0 CONCLUSION

The BCUC is concerned about the risks that cybersecurity threats pose to public utilities in BC and conducted a high-level survey to assess the level of preparedness to mitigate the risks. The BCUC evaluated multiple alternatives and cybersecurity standards and frameworks and is of the view that the NIST Cybersecurity Framework is suitable for adoption by public utilities for their Applicable Systems.

6.0 APPENDIX A: CYBERSECURITY IN OTHER JURISDICTIONS

This section provides an overview of how cybersecurity is addressed for public utilities and other critical energy sectors. The review includes a search for cybersecurity regulation or practices in other Canadian provinces and territories, at the federal level, related energy sectors such as oil and gas and other regions in North America. This is only a sample of jurisdictions; there are many more that are not included.

Cybersecurity requirements for entities vary widely by jurisdiction. The NERC Critical Infrastructure Protection (CIP) standards are the only mandatory standards in each jurisdiction. Ontario has facilitated the development of a Cybersecurity and Privacy Framework that is recommended for their electrical distribution entities. The Ontario Energy Board requires reporting by these entities at a high level.

Massachusetts and Connecticut have developed a cybersecurity reporting framework in consultation with impacted entities.

6.1 NERC Critical Infrastructure Protection (CIP) Standards

NERC is the Electric Reliability Organization (ERO) for North America, as designated by the Federal Energy Regulatory Commission (FERC) and recognized by Canadian provinces. NERC develops and publishes the Critical Infrastructure Protection (CIP) standards that specify the cybersecurity compliance requirements for applicable Bulk Electric System (BES) Cyber Systems. Public utilities and other entities in Canada are required to comply with the NERC CIP standards for cyber systems that are associated with BES Facilities. MRS Registrants in BC are required to comply with applicable NERC CIP requirements based on the Impact Level of their BES Cyber Systems.

The NERC reliability and cybersecurity standards apply mostly to generation systems over a certain threshold, high voltage transmission systems (over 100 kV) and Control Centers; thus, most local low voltage distribution systems are excluded.

Cybersecurity is specifically addressed in the MRS through the NERC Critical Infrastructure Protection (CIP) standards listed below. The standards versions are current as of the writing of this report. Newer versions may be available in future.

Standard Name	Title	Purpose
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization	To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES.

Standard Name	Title	Purpose
CIP-003-8	Cyber Security — Security Management Controls	To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-004-6	Cyber Security — Personnel & Training	To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems.
CIP-005-6	Cyber Security — Electronic Security Perimeter(s)	To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-006-6	Cyber Security — Physical Security of BES Cyber Systems	To manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.
CIP-007-6	Cyber Security — System Security Management	To manage system security by specifying select technical, operational, and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-008-5	Cyber Security — Incident Reporting and Response Planning	To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
CIP-009-6	Cyber Security — Recovery Plans for BES Cyber Systems	To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
CIP-010-2	Cyber Security — Configuration Change Management and Vulnerability Assessments	To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the Bulk Electric System (BES).
CIP-011-2	Cyber Security — Information Protection	To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the Bulk Electric System (BES).

Standard Name	Title	Purpose
CIP-012-1 [12]	Cyber Security – Communications between Control Centers	To protect the confidentiality and integrity of Real-time Assessment and Real-time monitoring data transmitted between Control Centers.
CIP-013-1 [13]	Cyber Security - Supply Chain Risk Management	To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems.
CIP-014-2	Physical Security	To identify and protect Transmission stations and Transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection.

The NERC Standard Numbering System[14] describes the naming of the NERC standards.

6.2 Ontario Cybersecurity Framework

The Ontario Energy Board (OEB) mandate[15] is established by the provincial government and is embodied in legislation, regulation and directives. In November 2010, the Minister of Energy issued a Directive to the Board in relation to the implementation and promotion of the Smart Grid in the Province. The Board was guided by ten (10) government policy objectives, which included security and privacy as two key objectives as follows:

> v. *Security*: Cyber security and physical security should be provided to protect data, access points, and the overall electricity grid from unauthorized access and malicious attacks; and
>
> vi. *Privacy*: Respect and protect the privacy of customers. Integrate privacy requirements into smart grid planning and design from an early stage, including the completion of privacy impact assessments.

The OEB issued a letter on February 11, 2016, to the IESO and all licensed electricity market participants in Ontario, inviting participation in an initiative for "Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario".[16] The project scope was restricted to the non-bulk electric system and associated business systems; i.e., the electricity facilities that are not in scope of the NERC Critical Infrastructure Protection (CIP) standards. The OEB established a Cyber Security Steering Committee and a Cyber Security Working Group to oversee and execute the project. The OEB also retained consultants to work on the project.

[12] Will be effective on October 1, 2023
[13] Will be effective on April 1, 2023
[14] https://www.nerc.com/pa/Stand/Resources/Documents/NERC_Standards_Numbering_System.pdf
[15] https://www.oeb.ca/about-oeb/mission-and-mandate
[16] https://www.rds.oeb.ca/CMWebDrawer/Record/516630/File/document

On June 1, 2017 the OEB issued a Staff Report to the Board on a Proposed Cyber Security Framework and Supporting Tools for the Electricity and Natural Gas Distributors, and the accompanying industry-developed Cyber Security Framework.[17] The OEB received comments on the proposed Cyber Security Framework from electric and gas utilities and industry bodies.

On December 20, 2017, the OEB issued a Proposed Notice of Code Amendments for the Electricity and Natural Gas Distributors,[18] and the accompanying industry-developed Ontario Cyber Security Framework, tools and Framework Implementation Report. The OEB received comments from impacted entities.

On March 15, 2018, the OEB issued a Notice of Amendments to the Distribution System Code and the Transmission System Code to implement the OEB's policies related to Protecting Privacy of Personal Information and the Reliable Operation of the Smart Grid in Ontario for the Electricity and Natural Gas Distributors. Mandatory reporting requirements were implemented.

A complete record of the project is available at the project web site.[19]

It may be noted that the OEB combined cybersecurity and privacy controls into a single framework.

6.3 Massachusetts Department of Public Utilities

The Massachusetts Department of Public Utilities (DPU)[20] oversees investor-owned electric power, natural gas, and water companies in Massachusetts. In addition, the DPU regulates the safety of bus companies, moving companies, and transportation network companies. They also oversee the safety of natural gas pipelines.

In 2014, the DPU issued a request for a joint proposal from the state's gas and electric distribution companies outlining a framework for how the Department should review the companies' cybersecurity preparedness. The electricity and gas companies submitted a joint proposal that was reviewed by the Department. A memorandum was issued by the DPU to all companies in 2015, with amendments to the original joint proposal that was adopted as the cybersecurity framework. This framework has been amended as necessitated over the years.

The DPU cybersecurity program documentation is non-public.

[17] https://www.oeb.ca/sites/default/files/Staff-Report-Cyber-Security-Framework-20170601.pdf
[18] https://www.rds.oeb.ca/CMWebDrawer/Record/594480/File/document
[19] https://www.oeb.ca/industry/policy-initiatives-and-consultations/protecting-privacy-personal-information-and-reliable
[20] https://www.mass.gov/orgs/department-of-public-utilities

6.4 State of Connecticut Public Utilities Regulatory Authority

In 2013, the Connecticut General Assembly ratified the "2013 Comprehensive Energy Strategy for Connecticut" [21], prepared by the Connecticut Department of Energy and Environmental Protection (DEEP). The Public Utilities Regulatory Authority (PURA) was directed to review the state's electricity, natural gas and major water companies and to assess the adequacy of their capabilities to deter interruption of service and to present to the Governor and General Assembly recommended actions to strengthen deterrence. The PURA published their report on "Cybersecurity and Connecticut's Public Utilities" [22] in April 2014.

The PURA report identifies a number of basic questions that should be discussed with utilities to determine where concurrence exists and where further discussion is required. Questions were grouped in the following broad categories:

1. Performance criteria
2. Role of regulators
3. Consistency of state regulation
4. Reporting on cyber threats
5. Information sharing
6. Confidentiality
7. Personnel security
8. Reporting standards
9. Municipal utility oversight
10. Cost / benefit considerations
11. Training and exercise
12. Emergency management

The PURA conducted a number of technical meetings with the utilities. Based on the discussions PURA established a Cybersecurity Oversight Program for each of the three industries that agreed to participate: electricity, gas and water utilities. The Oversight Program envisioned annual voluntary cybersecurity review meetings with attendees restricted on a need-to-know basis. The topics deemed appropriate for the meetings include:

1. Management's commitment to cybersecurity
2. Company's culture of cybersecurity
3. Cybersecurity program status
4. Engagement with external cyber expertise
5. Results of recent third-party security assessments
6. Technical review of cybersecurity program and practices

Confidentiality measures were specified to protect sensitive information.

The PURA has published an annual public utility cybersecurity report since 2017. All reports are available at https://portal.ct.gov/PURA/Electric/Cybersecurity-and-Connecticut-Public-Utility-Companies. The reports are fairly general in nature.

[21] https://portal.ct.gov/-/media/DEEP/energy/CEP/2013CESFINALpdf.pdf
[22] https://portal.ct.gov/-/media/DAS/BEST/Security-Services/Cybersecurity-and-Connecticuts-Public-Utilities.pdf

6.5 Government of Canada Bill C-26

On June 14, 2022, the Government of Canada introduced Bill C-26, An Act Respecting Cyber Security (ARCS). [23,24] ARCS would enact the Critical Cyber Systems Protection Act, which would establish a regulatory framework to strengthen baseline cybersecurity for services and systems that are vital to national security and public safety and gives the Government a new tool to respond to emerging cyber threats. It would also introduce a regulatory regime requiring designated operators in the finance, telecommunications, energy and transportation sectors to protect their critical cyber systems. This is in addition to proposed amendments to the Telecommunications Act, which are also part of the Bill.

The legislation enables the government to:

- designate services and systems that are vital to national security or public safety in Canada as well as the operators or classes of operators responsible for their protection;
- ensure that designated operators are protecting the cyber systems that underpin Canada's critical infrastructure;
- ensure that cyber incidents that meet or exceed a specific threshold are reported;
- compel action by organizations in response to an identified cyber security threat or vulnerability; and
- ensure a consistent cross-sectoral approach to cyber security in response to the growing interdependency of cyber systems.

This legislation will apply to designated operators of federally regulated services and systems in four priority sectors: finance, energy, telecommunications, and transport. Vital services and systems in each of these four sectors include:

- telecommunications services;
- interprovincial or international pipeline and power line systems;
- nuclear energy systems;
- transportation systems that are within the legislative authority of Parliament;
- banking systems; and
- clearing and settlement systems.

[23] https://www.canada.ca/en/public-safety-canada/news/2022/06/protecting-critical-cyber-systems.html
[24] https://www.parl.ca/legisinfo/en/bill/44-1/c-26

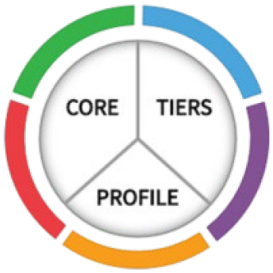
7.0 APPENDIX B: CYBERSECURITY STANDARDS, FRAMEWORKS AND GUIDELINES

This section is an overview of cybersecurity standards, frameworks and guidelines published by government agencies, industry bodies and standards making bodies.

A cybersecurity standard is a structured set of cybersecurity controls that is adopted by an organization to mitigate cybersecurity risks addressed by the controls. A cybersecurity guideline is more informal guidance on the implementation of cybersecurity. Standards may be mandatory or voluntary; for example, the NERC Critical Infrastructure Protection (CIP) standards are mandatory for all applicable entities; whereas the NIST Cybersecurity Framework (CSF) was developed as a voluntary framework.

Cybersecurity standards are published by governments, industry associations and standards making bodies. They can be generic as in being applicable to a wide range of industries or they could be specific to an industry, for example, for the oil and gas sector.

7.1 NIST Cybersecurity Framework



The Cybersecurity Framework (Framework)[25] published by the National Institute of Science and Technology (NIST) is a voluntary framework that can be customized and implemented by small to large organizations in different industry segments. The Framework comprises a Framework Core, Implementation Tiers and Profiles.

The Framework **Core** provides a set of desired cybersecurity activities and outcomes using common language that is easy to understand. The Core guides organizations in managing and reducing their cybersecurity risks in a way that complements an organization's existing cybersecurity and risk management processes.

The Framework Core comprises five **Functions** that organize cybersecurity activities at the highest level. These are:

- Identify
- Protect
- Detect
- Respond
- Recover

Each Function is subdivided into **Categories** that are groups of logically related cybersecurity activities. For example, the Identify Function has the following Categories:

[25] https://www.nist.gov/cyberframework

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Management

Subcategories are specific cybersecurity outcomes of activities related to the Category. Examples of Subcategories in the Asset Management Category include:

- Physical devices and systems within the organization are inventoried
- Software platforms and applications within the organization are inventoried
- Organizational communication and data flows are mapped
- External information systems are catalogued
- Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
- Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Another example of the subcategories for the category "Business Environment" is shown below.

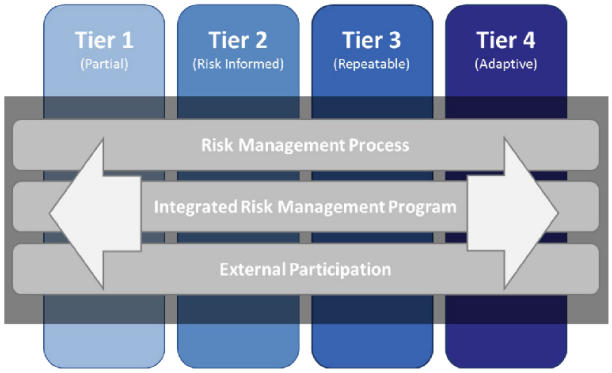
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Each subcategory includes **Informative References** that are established industry cybersecurity standards. Informative References linked to a subcategory further enhance the subcategory requirements by specifying additional requirements to support the desired outcomes of the subcategory. Informative References are optional and may be mixed and matched across subcategories.

The Framework **Implementation Tiers** assist organizations by providing context on how an organization views cybersecurity risk management. The Tiers guide organizations to consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.

The four Implementation Tiers are:



Tiers do not necessarily represent maturity levels. Organizations should determine the desired Tier, ensuring that the selected level meets organizational goals, reduces cybersecurity risk to levels acceptable to the organization, and is feasible to implement, fiscally and otherwise.

A Framework **Profile** is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal and regulatory requirements and industry best practices, and reflects risk management priorities.

Examples of Framework Profiles[26] for diverse industry applications are available to use as is or to customize for specific applications. NISTIR 8183 Revision 1 Cybersecurity Framework Version 1.1 Manufacturing Profile[27] has been created specifically for the manufacturing sector.

7.2 NIST SP-800-53 Security and Privacy Controls for Information Systems and Organizations

NIST Special Publication 800-53 (SP-800-53)[28] provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals and organizations from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. The controls are flexible and customizable and implemented as part of an organization-wide process to manage risk. The control catalog addresses security and privacy from a functionality perspective (i.e., the strength of functions and mechanisms provided by the controls) and from an assurance perspective (i.e., the measure of confidence in the security or privacy capability provided by the controls). Addressing functionality and assurance helps to ensure that information technology products and the systems that rely on those products are sufficiently trustworthy.

[26] https://www.nist.gov/cyberframework/examples-framework-profiles
[27] https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf
[28] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

7.3 SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security

NIST Special Publication 800-82 Rev. 2 (SP 800-82 Rev. 2)[29] provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

Industrial Control Systems are critical to the safe and reliable operation of industrial processes and require special cybersecurity considerations that may be different from cybersecurity for IT systems.

7.4 CIS Critical Security Controls

The Center for Internet Security Critical Security Controls[30] (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks.

Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the CIS Controls. Three Implementation Groups have been defined to assist enterprises of every size. They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls. Each Implementation Group identifies a set of Safeguards that are required to be implemented.

7.5 CISA Cyber Essentials Starter Kit

The Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials[31] is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. Consistent with the NIST Cybersecurity Framework and other standards, the Cyber Essentials are the starting point to cyber readiness.

7.6 ISA/IEC 62443 Series of Standards

The ISA/IEC 62443[32] series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of security performance. Their approach to the cybersecurity challenge is a holistic one, bridging the gap between operations and information technology as well as between process safety and cybersecurity.

The ISA/IEC standards set cybersecurity benchmarks in all industry sectors that use IACS, including building automation, electric power generation and distribution, medical devices, transportation, and process industries such as chemicals and oil and gas.

[29] https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
[30] https://www.cisecurity.org/controls
[31] https://www.cisa.gov/publication/cisa-cyber-essentials
[32] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

7.7 ISO/IEC 27001 Information Security Management

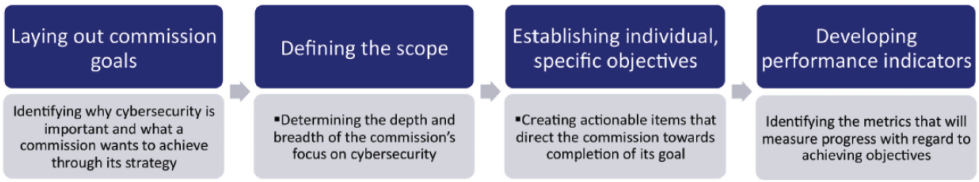
ISO/IEC 27001:2013[33] specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. The requirements set out in ISO/IEC 27001:2013 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.

7.8 CSA Z246.1:21 Security management for petroleum and natural gas industry systems

CSA Z246.1[34] 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.

7.9 NARUC Cybersecurity Strategy Development Guide

In 2018 the National Association of Regulatory Utility Commissioners (NARUC) published the Cybersecurity Strategy Development Guide[35] to provide guidance and practices to state public utility commission (PUC) regulators in developing cybersecurity strategies for their commissions. The guide suggests initial steps in the development process.



The guide includes a sample template structure for a cybersecurity plan with the following sections:

1. Develop Strategic Goal
2. Define Scope
3. Identify Cybersecurity Needs and Develop Objectives
4. Establish Performance Indicators
5. Identify Key Stakeholders
6. Determine Resource Needs
7. Develop a Communication Plan
8. Implement Strategy
9. Review Progress

[33] https://www.iso.org/standard/54534.html
[34] https://www.csagroup.org/store/product/CSA%20Z246.1%3A21/
[35] https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204

7.10 National Conference of State Legislatures

The National Conference of State Legislatures (NCSL)[36] represents the legislatures in the states, territories and commonwealths of the US. The NCSL promotes interstate cooperation among state legislatures and also represents legislatures in dealing with the federal government on various matters.

The NCSL published a research document "Cybersecurity and the Electric Grid | The state role in protecting critical infrastructure" [37] in January 2020, that provides a comprehensive overview of what the states have done to reinforce cybersecurity for gas utilities and electricity systems other than the bulk power system. The actions described fall into the following four categories:

- Establishing state-level cybersecurity task forces and committees.
- Establishing cybersecurity standards and reporting requirements.
- Expanding state open records exemptions to include cyber vulnerabilities.
- Directing and authorizing governors and state agencies to take certain actions to prepare for and respond to cyber emergencies.

The document also addresses issues of financing cybersecurity programs for utilities. While the traditional rate case is utilized for significant cybersecurity funding, some states like Minnesota have provided funding for grid modernization that can be used for cybersecurity along with other modernization actions.

[36] https://www.ncsl.org/
[37] https://www.ncsl.org/research/energy/cybersecurity-and-the-electric-grid-the-state-role-in-protecting-critical-infrastructure.aspx

8.0 ATTACHMENT 1: INFORMATION BULLETIN 21-01

bcuc
British Columbia Utilities Commission

Suite 410, 900 Howe Street
Vancouver, BC Canada V6Z 2N3
bcuc.com

P: 604.660.4700
TF: 1.800.663.1385
F: 604.660.1102

21-01

INFORMATION BULLETIN 21-01 – Regulated Entities and Cybersecurity

February 8, 2021

In recent months, utilities and energy sectors have experienced increased activity and risk related to cybersecurity.

In late 2020, critical infrastructure providers, including utilities, became aware of a cyberattack that planted malicious code in certain SolarWinds software to create a backdoor entrance to its customers. Further, in February 2021, Powertech Labs, a research-based entity and wholly owned subsidiary of British Columbia Hydro and Power Authority (BC Hydro), experienced a cyber-attack targeting data held by the company. In addition, various utility operators have seen ongoing attempts to gain direct access to their cyber systems. If successful, these cyber-attacks grant system access to hackers who can then extract data and install malware or ransomware.

The British Columbia Utilities Commission (BCUC) considers cyber risk a significant threat to all regulated entities in British Columbia. The likelihood of experiencing a successful cyberattack is increasing. As such, the BCUC expects all regulated entities to mitigate cyber exposure and establish a plan to respond effectively in the event of a cyber-attack.

All entities should be vigilant in protecting customer information, operating data and system controls from any threat, including a potential cyber-attack. Regulated entities should perform a thorough and appropriate cybersecurity vulnerability assessment on their operations, have a detailed and tested disaster recovery plan and ensure adequately skilled resources are available to execute the recovery plan in the event of an attack. Regular monitoring of systems should be conducted to detect any cyberbreaches that may have occurred.

Various resources are available to support regulated utilities in assessing and addressing cyber risk and cyberattack. The leading organizations in cybersecurity for the utility and energy industries in Canada and North America are listed below. The BCUC reminds regulated entities of their obligations to provide safe and reliably services to customers and as such, strongly encourages all regulated entities to review these links and implement appropriate recommendations:

- **The Canadian Center for Cybersecurity** offers various services related to cybersecurity. Its website provides updates on current threats, tools for cybersecurity vulnerability self-assessment, best practices for cyber-protections and disaster recovery planning. Canadian entities can register for additional services including planning & monitoring support, tailored risk notifications, and access to other industry support to address cyber risk and recovery.

  A link to learn more is found here: https://cyber.gc.ca/en/