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

British Columbia Utilities Commission

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

---

Decision and Order G-126-23

June 2, 2023

Before:
D. M. Morton, Commissioner

TABLE OF CONTENTS

Page no.

Executive Summary

On December 23, 2022, the British Columbia Utilities Commission (BCUC) issued a proposed cybersecurity framework for public utilities (Cybersecurity Framework) and established a comment process regarding a two-year pilot of the Cybersecurity Framework (Pilot). The Cybersecurity Framework is based on the National Institute of Standards and Technology Cybersecurity Framework Version 1.1 and is flexible and scalable based on the size and risk profile of the public utility and makes use of existing industry guidance. The purpose of the Pilot is to assess the effectiveness of the Cybersecurity Framework to address public utility cybersecurity risk.[1]

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

i) establishment of the Pilot;

ii) the proposed Cybersecurity Framework; and

iii) a proposed annual cybersecurity declaration (Annual Declaration).

The BCUC received eight letters of comment from public utilities, indicating support for the Pilot and requesting certain clarifications and revisions to the Cybersecurity Framework and the Annual Declaration.

The Panel has considered the comments received and concludes that establishment of the Pilot is warranted. The Panel finds that with certain revisions the proposed Cybersecurity Framework and Annual Declaration are appropriate for use in the Pilot and adopts the versions of these documents attached as Appendix A and Appendix B to this Decision as final.

The Panel also finds that an effective date of January 1, 2024, is appropriate for the Pilot. Public utilities are directed to file two progress reports in advance of this effective date, on September 1, 2023 and November 1, 2023. The progress reports are to contain, at a minimum, an attestation by the public utility of its commitment to meeting the January 1, 2024 effective date and documentation of the public utility's progress towards implementation. Further, public utilities are required to file a copy of the Annual Declaration on or before January 1, 2024, confirming implementation of the Cybersecurity Framework.

The BCUC will consider adopting the Cybersecurity Framework on a permanent basis after completion of the Pilot.

[1] Order G-385-22.

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 has general supervision of all public utilities[2] pursuant to section 23 of the 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.

In January 2022, BCUC staff conducted a high-level survey of the cybersecurity preparedness of public utilities in BC. The results of this survey indicated significant variance in the ability of public utilities to mitigate cybersecurity risk.[3] The BCUC has also observed increasing rates and severity of cyber-attacks globally and within Canada, and significant costs to recover from cybersecurity incidents.

On December 23, 2022, the BCUC issued a proposed framework to address cybersecurity risk for public utilities (Cybersecurity Framework) as well as a proposed annual cybersecurity declaration for public utilities (Annual Declaration). The Cybersecurity Framework is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) Version 1.1 and is flexible and scalable based on the size and risk of the public utility and makes use of existing industry guidance.

The BCUC proposed introducing the Cybersecurity Framework and Annual Declaration on a two-year pilot basis to assess its effectiveness in addressing public utility cybersecurity risk (Pilot).

2.0 Regulatory Process

On December 23, 2022, the BCUC issued Order G-385-22 and established a comment process. Public utilities were invited to provide submissions on the following:

i) establishment of the Pilot;

ii) the Cybersecurity Framework; and

iii) the Annual Declaration.

By March 2, 2023, the BCUC received written comments from the following public utilities:

- British Columbia Hydro and Power Authority (BC Hydro);
- Corix Multi-Utility Services Inc. (Corix);
- FortisBC Energy Inc., FortisBC Inc., and FortisBC Alternative Energy Services Inc. (collectively FortisBC);
- Nelson Hydro;
- Pacific Northern Gas (PNG);
- River District Energy (RDE);

[2] 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.

[3] Order G-385-22, Appendix C Cybersecurity Technical Report.

- Silversmith Power & Light Corporation (Silversmith); and
- Sustainable Services Limited (SSL)

3.0 Establishment of the Pilot

Positions of the Parties

Commentors wrote in support of the Pilot, noting the critical importance of mitigating cybersecurity risks to BC's public utilities.[4]

For instance, PNG states that it is supportive of the establishment of a two-year pilot of a cybersecurity framework for public utilities, and that "PNG believes that a strong cybersecurity program with appropriate processes and measures are (sic) critical for all entities in the current geopolitical environment."[5] Corix submits that implementation of the Pilot is reasonable and appropriate, and that the two-year timeline should provide sufficient time for public utilities to plan and implement changes to their cybersecurity program, if required.[6]

Nelson Hydro states that it is pleased to see that the Pilot provides a flexible and scalable framework based on the size and risk exposure of the public utility.[7] Silversmith states that while its utility operations would not be impacted directly by a cyber-attack, its service and customers could be impacted if a cyber-attack on its interconnected public utility BC Hydro isolated Silversmith from the BC Hydro electrical network. As such, cybersecurity is also of concern to Silversmith.[8]

While RDE does not object to implementation of the Pilot itself, in its comments RDE expresses concern that the NIST CSF Version 1.1 may not be the most appropriate framework to adopt. RDE notes that the NIST is currently developing version 2.0 of its cybersecurity framework, and that the planned winter 2024 release date overlaps with the proposed Pilot period. RDE recommends that the BCUC consider timing the Pilot to take into account the anticipated updates to the NIST CSF. Further, RDE submits that if the BCUC plans to continue to use the NIST CSF Version 1.1 past the release of CSF Version 2.0 "this must be explicitly made clear, and a rationale presented for doing so."[9] RDE states that it is concerned that there may be significant regulatory inefficiency if public utilities are expected to manage cybersecurity using two different, although related, frameworks to meet the different cybersecurity needs and expectations of different stakeholders.[10]

BC Hydro and FortisBC note that any incremental one-time or ongoing costs associated with implementation of the Pilot would be brought forward to the BCUC in upcoming filings, if such costs could not be absorbed into existing operating budgets.[11] Corix recommends that the BCUC consider cost recovery of the Pilot on a case-by-case basis and suggests that the use of temporary deferral accounts and rate riders may be appropriate in certain circumstances.[12]

Finally, in its comments, SSL states that one way to support a successful outcome for the Pilot would be for the BCUC to provide dedicated subject matter experts to liaise with public utilities and provide informal guidance.[13]

---

[4] Exhibit E-1, p. 1; Exhibit E-2, p. 1; Exhibit E-3, p. 1; Exhibit E-4, p. 1; Exhibit E-5, p. 1; Exhibit E-6, p. 1; Exhibit E-7, p. 1; Exhibit E-8, p. 2.
[5] Exhibit E-8, p. 2.
[6] Exhibit E-7, p. 1.
[7] Exhibit E-5. P. 1.
[8] Exhibit E-1, p. 1.
[9] Exhibit E-2, p. 2.
[10] Ibid.
[11] Exhibit E-4, p. 2. Exhibit E-6, p. 3.
[12] Exhibit E-7, p. 1.
[13] Exhibit E-3, p. 1.

Panel Determination

The Panel notes the unanimous support of commentors for the Pilot and **finds that the establishment of a two-year Pilot of the Cybersecurity Framework and Annual Declaration is warranted**. The BCUC will consider whether to adopt the Cybersecurity Framework on a permanent basis after completion of the Pilot.

The Pilot will be effective January 1, 2024, to allow sufficient time for public utilities to implement the Cybersecurity Framework. The Panel is aware that work to develop the NIST CSF Version 2.0 is in progress; however the Panel is not persuaded that any benefits associated with delaying the Pilot until after Version 2.0 is released (a final date for which remains uncertain) outweigh the need for prompt action to mitigate cybersecurity risks to BC's public utilities. An update from NIST CSF Version 1.1 to Version 2.0 may be considered after the Pilot is completed, coincident with an evaluation of the effectiveness of the Pilot itself. Section 5.0 of the Cybersecurity Framework has been amended to include the following explanation of the versioning convention for the BC Cybersecurity Framework:

> The version of the BC Cybersecurity Framework will follow the version of the adopted NIST Cybersecurity Framework, with an uppercase letter appended to denote the BC release. The initial version of the BC Cybersecurity Framework is Version 1.1A. Any subsequent revisions to the BC framework, based on the NIST Cybersecurity Framework Version 1.1 will be Version 1.1B, 1.1C, and so on.

To support effective communication and BCUC oversight in the period leading up to the Pilot effective date, public utilities must file two progress reports with the BCUC, the first on September 1, 2023, and the second on November 1, 2023. The progress reports are to contain, at a minimum, an attestation by the public utility of its commitment to meeting the January 1, 2024 effective date and documentation of the public utility's progress towards implementation. Further, public utilities must file a copy of the Annual Declaration on or before January 1, 2024, confirming implementation of the Cybersecurity Framework.

The Panel sees merit in SSL's submission that access to subject matter experts within the BCUC would support the success of the Pilot. Relevant BCUC staff will be made available, as appropriate, to support public utilities throughout the Pilot. Further, the BCUC will issue implementation guidance from time to time on the Cybersecurity Framework to guide public utilities in their cybersecurity program development and implementation.

Finally, regarding the recovery of costs associated with the Pilot, the BCUC will consider the merits of any requests following application by a public utility.

4.0 Cybersecurity Framework

With respect to the proposed Cybersecurity Framework itself, with the exception of the areas noted below, commentors were supportive of, or provided no comments on, the proposed language of the framework and the Panel adopts the language as final. A copy of the final Cybersecurity Framework is attached as Appendix A to this decision. A blacklined copy showing the changes from the original proposal is attached as Appendix C.[14]

[14] The Panel notes that in addition to the revisions discussed in Sections 4.1 to 4.4, below, the language in the final Cybersecurity Framework has also been updated for non-substantive improvements. All changes are marked in the blacklined copy of the final framework provided in Appendix C.

4.1 Terms and Definitions and Applicability

Sections 2.0 and 3.0 of the Cybersecurity Framework set out a list of terms and definitions used in the Cybersecurity Framework and describe the scope of the framework.

Positions of the Parties

BC Hydro submits that the proposed framework would benefit from a more narrowly defined scope and that the definitions of the terms Applicable Systems, Critical Cyber Asset and Service are ambiguous. BC Hydro recommends further clarifying these definitions so that public utilities can identify and categorize their systems according to the risk-based approach used by the NIST CSF.[15]

Corix submits that Section 2.0 should include a definition of the term "cybersecurity information", which is used in the Cybersecurity Framework and the Annual Declaration.[16]

Corix also requests clarification as to whether the Cybersecurity Framework is applicable to Stream A Thermal Energy Systems (TES) as defined by the BCUC.[17]

Panel Determination

The Panel adopts sections 2.0 and 3.0 of the proposed Cybersecurity Framework as final along with the revisions discussed below.

The Panel notes BC Hydro's concerns about the non-prescriptive nature of the terms Applicable Systems, Critical Cyber Asset, and Service in the proposed Cybersecurity Framework. Some ambiguity was purposefully included in these definitions to allow public utilities latitude and discretion when identifying the core aspects of their systems that need to be protected from cybersecurity threats. Nevertheless, the Panel is persuaded that the proposed language would benefit from certain revisions to the definitions and elimination of one term.

The term "Applicable Systems" is deleted and the term "Critical Cyber System" is revised to identify devices and systems in scope of the Cybersecurity Framework. The revised definition is as follows:

> 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. Critical Cyber Systems exclude BES Cyber Systems.

The term "Critical Cyber Asset" has been revised to clarify that this may be a physical asset or a virtual asset such as a virtual machine or a container. Public utilities are advised to assess the adequacy of the security of the underlying virtualization infrastructure that may be owned by the public utility or by a third party such as the public utility's parent entity or a cloud services provider. The revised definition is:

> Critical Cyber Asset: A cyber asset that, if its availability, integrity or confidentiality were degraded or compromised, could adversely impact the Service of the public utility. A Critical Cyber Asset may be a physical device or a virtual device, for example, a container, virtual server or virtual firewall. This includes redundant and standby devices.

[15] Exhibit E-4, pp. 2-3.
[16] Exhibit E-7, p. 2.
[17] Exhibit E-7, p. 3.

The definition of the term "Service" in the Cybersecurity Framework is revised to focus on 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. This definition provides guidance to public utilities in identifying the plant, equipment, apparatus, appliances, property and facilities employed by or in connection with a public utility in providing Service. The revised definition is:

> Service: 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.

The Panel is also persuaded by Corix's submission that including a definition for "cybersecurity information" would improve the clarity of the Cybersecurity Framework. Accordingly, the following definition is added:

> Cybersecurity Information: Non-public information about Critical Cyber Systems and their components that could be misused by an adversary to gain unauthorized access to Critical Cyber Systems to adversely impact the Service of the public utility. Cybersecurity information includes, but is not limited to, cyber asset configuration, physical and electronic access control systems configuration, network information, backup and restoration plans, incident response plans, security monitoring information and physical plant layout drawings.

With these revisions, it is clear that the scope of the Cybersecurity Framework includes digital or electronic devices and systems that are necessary to monitor or control the "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". These devices and systems may be physical or virtual, may be owned by the public utility or by an associated or parent entity and may be hosted on the public utility's own infrastructure or on infrastructure owned by the parent or associated entity or a third-party infrastructure provider.

The Panel notes that there may be other devices or systems that may indirectly monitor or control such equipment or facilities or monitor or control access to such equipment or facilities. Public utilities are advised to identify such devices or systems as well and include them in the scope of the Cybersecurity Framework if deemed material to the safety and adequacy of their Service.

Public utilities are also advised to assess the risks of interconnected IT or OT systems that are not Critical Cyber Systems and to implement adequate protection for these systems to prevent them from being used as conduits to attack or compromise Critical Cyber Systems.

Finally, regarding Corix's request for clarification as to whether Stream A TES are captured within the scope of the Pilot, the Panel considers it to be appropriate to limit the scope of the Pilot to Stream B TES only, as these are the systems most actively regulated by the BCUC. Following completion of the Pilot consideration will be given as to whether the Cybersecurity Framework is appropriate for adoption by other categories of TES and other public utilities with partial exemptions from the UCA. Section 3.0 of the Cybersecurity Framework has been revised accordingly to clearly indicate this.

4.2 Incident Reporting

Positions of the Parties

Section 5.0 of the Cybersecurity Framework sets out the implementation approach, including proposed timelines for public utilities to report cybersecurity incidents to the BCUC.

Corix recommends that the cybersecurity incident reporting timeframe be revised to be within two days of confirmation of an incident, instead of within two days of detection of an incident, because a detection may not result in a confirmed incident after subsequent investigation. Corix also submits that the BCUC should develop a streamlined reporting procedure or guideline regarding reporting cybersecurity incidents.[18]

RDE expresses its understanding that the BCUC included a reporting requirement so that the BCUC is aware of any incidents involving the public utilities it regulates, and not so that the BCUC will provide support or coordination to respond to an incident. RDE recommends that the requirement to report an incident be within a maximum of five business days, to allow public utilities to prioritize response over reporting. RDE further submits that cybersecurity incident information should be shared with other public utilities in a manner that would provide an early warning to them. RDE suggests that the BCUC publish a cybersecurity dashboard with anonymized information; and that the BCUC produce advisories for public utilities in a timely fashion on notable trends or specific threats. Finally, RDE also submits that the BCUC should require an after-action report within 60 days of the end of an incident.[19]

Panel Determination

The Panel adopts section 5.0 of the proposed Cybersecurity Framework as final along with the revisions discussed below in this section and in section 4.3.

The Panel has reviewed the comments and recommendations for cybersecurity incident reporting and information sharing and concludes that revisions to the language in the proposed Cybersecurity Framework are warranted.

The Panel concurs with Corix's submission that the BCUC should develop a streamlined reporting procedure or guideline to report cybersecurity incidents. Including this information in the Cybersecurity Framework will provide public utilities with clarity on the content and timing of reporting. Such reporting should be guided by the impact and severity of the incident.

The Panel is not persuaded by RDE's recommendation that the requirement to report an incident be within a maximum of five business days, to allow public utilities to prioritize response over reporting, as this may limit the BCUC's awareness of serious cybersecurity matters. However, the Panel sees value in Corix's recommendation that the cybersecurity incident reporting timeframe be revised to be within two days of confirmation of an incident to avoid unnecessary reporting of non-incidents, with certain adjustments to consider the impact and severity of the incident.

Public utilities are required to report incidents within timeframes appropriate for the impact and severity of the incident, to provide the BCUC early notification of the incident rather than a detailed report during the initial stage of the incident response. Potential security events not confirmed within five business days of detection must be reported to the BCUC for awareness as these may become confirmed incidents. Therefore, the Cybersecurity Framework is revised to include the following reporting procedure based on incident impact and severity:

a. Initial notification must be provided to the BCUC as soon as practicable by any means specified by the BCUC, for the following:
    (i) confirmation of a cybersecurity incident that impacted a Critical Cyber System and caused partial or total loss of production, generation, storage, transmission, sale, delivery or provision of any product or commodity in which the public utility is engaged; or

[18] Exhibit E-7, p. 2.
[19] Exhibit E-2, pp. 2-3.

(ii) confirmation of a physical security incident that posed a risk to a Critical Cyber System at a facility.

b. Initial notification must be provided to the BCUC by any means specified by the BCUC, within two business days of the following:
   (i) confirmation of a cybersecurity incident that impacted a Critical Cyber System but did not cause any loss of production, generation, storage, transmission, sale, delivery or provision of any product or commodity in which the public utility is engaged; or
   (ii) confirmation of an attempted physical security incident that posed a risk to a Critical Cyber System at a facility.

c. Initial notification must be provided to the BCUC of cybersecurity incidents or physical security events that could pose a risk to Critical Cyber Systems that are pending confirmation five business days after detection. Further notification must be provided if the incident is confirmed.

The Cybersecurity Framework now includes details on the minimum information expected to be reported by public utilities. Information may be added progressively to report updates as it becomes available. The public utility is expected to provide periodic updates, at least every month, until the incident is declared closed.

Further, the Panel concurs with RDE's view that inclusion of a requirement for an after-action report within 60 days of the end of the incident would strengthen the proposed Cybersecurity Framework. The proposed Framework has been revised accordingly.

The Panel recognizes that cybersecurity incident reports may contain sensitive information and advises public utilities to clearly mark such reports as being confidential.

The Panel confirms RDE's understanding that the BCUC expects public utilities to report cybersecurity incidents so that the BCUC is aware of the incidents and not so that the BCUC can participate as an incident response partner. Public utilities are advised to contact the Canadian Centre for Cyber Security (CCCS) or a professional cybersecurity incident response services organization for assistance with a cybersecurity incident, if needed.

The Panel appreciates RDE's suggestion that the BCUC establish a cybersecurity dashboard to share anonymized information on reported cybersecurity incidents with all public utilities as an early warning system. The Panel is not persuaded that a dashboard published by the BCUC is an effective method of sharing cybersecurity incident and threat information at this time. However, the BCUC will seek further inputs from public utilities on the merits of this proposal following completion of the Pilot. The Panel further recommends that public utilities subscribe to cybersecurity incident information sharing services offered by the CCCS, the Electricity Information Sharing and Analysis Centre and professional cybersecurity services organizations.

The Panel also appreciates RDE's suggestion to produce advisories for utilities on notable trends or specific threats. The BCUC intends to issue critical advisories to support public utilities in preparing for threats. However, ongoing advisories and alerts can be sourced from dedicated cybersecurity organizations that routinely collect, analyze and disseminate information on threats and incidents. Industry alerts, advisories and briefings on cybersecurity are available from the CCCS, the Electricity Information Sharing and Analysis Centre, the Cybersecurity and Infrastructure Security Agency and other professional cybersecurity services organizations. The Panel recommends that public utilities subscribe to these notifications and briefings.

4.3 Confidentiality and Data Storage, Retention and Security

Section 5.0 of the proposed Cybersecurity Framework also describes the data storage, retention and security requirements of cybersecurity information and the confidentiality of cybersecurity information collected by the BCUC from public utilities. The proposed framework requires public utilities to retain cybersecurity program review records and evidence of conformance for a minimum of five years. The proposed Cybersecurity Framework 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. Section 5.0 also proposes that the confidentiality of cybersecurity information collected by the BCUC will be determined by the BCUC's Rules of Practice and Procedure.

Positions of the Parties

RDE seeks clarification of the term "evidence of conformance" and requests the BCUC to provide specific examples. RDE submits that the completion of the Annual Declaration would provide sufficient confidence of conformance with the requirements. [20]

FortisBC and BC Hydro disagree with the BCUC recommendation that all cybersecurity information stored outside the public utility's premises and digital infrastructure reside within Canada. Both public utilities state that they have conducted security assessments of data storage infrastructure outside Canada and that these systems are a secure option.[21]

Finally, Corix submits that, by default, cybersecurity information collected by the BCUC should be held confidentially. Corix recommends that the confidentiality section in the Cybersecurity Framework be drafted in a manner that accounts for the uniqueness of this type of information instead of being tied to the BCUC Rules of Practice and Procedure.

Panel Determination

The Panel considers the term "evidence of conformance" to mean the evidence generated by Critical Cyber Systems and supporting tools, or documentation created to show that the cybersecurity requirements adopted by the public utility have been fulfilled.

The Panel recommends that public utilities use software tools to generate logs and reports as automated evidence where possible, and to create dated and signed policies, agreements, emails and review records as evidence where necessary. Examples of automated evidence includes firewall rules for electronic access controls, network scans and automated inventory tools to identify cyber assets, Windows security event logs, vulnerability scan reports, physical access control system access lists and access reports. Other evidence includes cybersecurity program documentation such as policies, procedures and work instructions, training and awareness communications and records, third-party service provider agreements and contracts. No changes to the proposed Cybersecurity Framework are necessary to support this clarification.

The Panel notes submissions by BC Hydro and FortisBC that data storage services outside Canada may be a secure option if an appropriate security assessment has been completed.[22] The Panel considers that there may be instances where storage systems outside of Canada can provide adequate protection to confidential information. Therefore Section 5.0 of the framework has been revised to include the following:

[20] Exhibit E-2, p. 3.
[21] Exhibit E-4, p. 3. Exhibit E-6, p. 2.
[22] Exhibit E-4, p. 3. Exhibit E-6, p. 2.

Public utilities are advised to conduct appropriate security assessments prior to transferring or storing their cybersecurity information outside Canada.

Finally, the Panel sees merit in Corix's submission that cybersecurity information collected from public utilities by the BCUC should be held confidentially, without the public utility bearing the onus of establishing that the cybersecurity information in question should be treated as such. This is consistent with accepted industry practice and is an appropriate reflection of the unique and highly sensitive nature of cybersecurity information. The confidentiality section in the Cybersecurity Framework is revised as follows:

All Cybersecurity Information submitted to the BCUC by public utilities will be considered confidential.

4.4 Annual Cybersecurity Declaration

Public utilities were invited to comment on the proposed Annual Declaration to be completed as part of the Pilot. The Annual Declaration must be signed by an officer of the public utility. The intent of the declaration is for the public utility to report its progress and status of implementation of key cybersecurity functions.

Positions of the Parties

BC Hydro notes that the NIST CSF uses the implementation tiers of "Partial", "Risk Informed", "Repeatable", and "Adaptive", whereas declarations 3 through 10 of the Annual Declaration provide the response options of "Yes", "No", or "Partial" when answering whether a cybersecurity function has been implemented. BC Hydro submits that the BCUC should consider replacing the "Yes", "No", and "Partial" with "Partial", "Risk Informed", "Repeatable", and "Adaptive" to allow for more accurate and consistent responses from participants that align with the NIST CSF-defined implementation tiers.[23]

As drafted, declaration 5 reads "Security updates are applied in a timely manner to all Critical Cyber System assets". BC Hydro and FortisBC state that security updates are not the only way to mitigate vulnerabilities, which may be adequately protected in other ways, such as network segregation, and recommend appending "where required to maintain accepted security levels" to the declaration.[24]

Declaration 7 requires that "[t]he public utility has contracts with third-party service providers that include cybersecurity terms and conditions". BC Hydro seeks clarification on whether contracts with third-party service providers is intended to refer to third-party service providers for Critical Cyber Systems specifically, or for all third-party service providers.[25]

As drafted, declaration 8 reads in part "Strong password policies are implemented". BC Hydro and FortisBC state that while it is best practice to implement password policies, not all assets support the use of complex or long passwords and, in particular, some Operational Technology assets do not use passwords to restrict access but may be adequately protected in other ways. These public utilities recommend appending "where technically feasible and required to restrict access" to this declaration.[26]

As drafted, declaration 9 reads "Malware detection and protection tools are installed on Critical Cyber Systems assets". BC Hydro and FortisBC state that not all assets support installation of malware detection and protection

[23] Exhibit E-4, pp. 3-4.
[24] Exhibit E-4, pp. 5-6. Exhibit E-6, pp. 2-3.
[25] Exhibit E-4, p. 4.
[26] Exhibit E-4, p. 4. Exhibit E-6, p. 3.

tools but may be adequately protected in other ways and recommend appending "where technically feasible and required to protect assets" to the declaration.[27]

Corix submits that the due date for the Annual Declaration should be changed from two months to four months after fiscal year end, to align with the deadline for public utility annual reports. Corix states that this alignment would streamline reporting for various compliance reports and promote efficiency.[28]

Corix further submits that the requirement to read and understand the entire UCA is onerous for the Authorized Signing Officer, and that for the purposes of this declaration, the BCUC should amend the declaration to include only the relevant sections of the UCA.[29]

FortisBC recommends an additional Cybersecurity Function (logically positioned following the existing Cybersecurity Function #3), that confirms the organization has a process to identify critical cyber assets because a process to identify what are critical cyber assets in the organization is necessary to support the risk management process associated with a reasonable cybersecurity program.[30]

The Annual Declaration Instruction 4 to fill the form states that public utilities may attach confidential information in a separate document, if required, clearly marked as confidential. BC Hydro and FortisBC submit that sharing their confidential cybersecurity information with the BCUC would create unnecessary risk and recommend that the BCUC implement an alternative process to share confidential information, such as through meetings.[31]

Finally, BC Hydro submits that the declaration instructions (3) and (4) are unclear and should be removed.[32]

Panel Determination

The Panel adopts the Annual Declaration as final with the revisions as noted below.

The Panel considers that BC Hydro's submission that "Partial", "Risk Informed", "Repeatable", and "Adaptive" responses be used in the declaration instead of "Yes", "No" and "Partial", is not appropriate for the Annual Declaration, since the Implementation Tiers of the NIST CSF reflect an organization's approach to risk management rather than the actual implementation of cybersecurity functions. The Panel also notes that in some circumstances public utilities may elect to implement cybersecurity standards or frameworks other than the NIST CSF, in which case the Implementation Tiers may not map to their selected framework. Therefore, the Panel declines to make this recommended change.

Regarding declaration 5, the Panel appreciates that security updates, or patches, are not the only way to mitigate vulnerabilities. However, patching is an essential layer in the defence-in-depth model for cybersecurity and high-risk critical cyber assets are expected to be patched where feasible. Network segregation is not necessarily an effective substitute for patching because attackers have demonstrated their ability to laterally traverse internal networks.

The Panel recognizes that patching may be burdensome to public utilities that have large numbers of cyber assets and not all vulnerabilities pose the same risk of exploitation. We recommend that public utilities install

[27] Ibid.
[28] Exhibit E-7, p.3.
[29] Ibid.
[30] Exhibit E-6, p. 3.
[31] Exhibit E-4, p. 4. Exhibit E-6, p. 3.
[32] Exhibit E-4, pp. 4-5.

security updates to high-risk Critical Cyber System assets where operationally and technically feasible. Public utilities may determine that cyber assets are not patched where the assessed risk of an unpatched vulnerability is deemed low or insignificant and compensating measures are implemented to mitigate risks. Exceptions to patching should be documented along with reasons and compensating measures implemented. Accordingly, declaration 5 is revised to read as follows:

> Security updates are applied in a timely manner to Critical Cyber System assets where feasible and required to maintain accepted security levels.

For declaration 7, the Panel confirms that the scope of the declaration includes contracts with third-party service providers for Critical Cyber Systems and related services, at a minimum, and that public utilities are advised to review other contracts as per perceived risks to Critical Cyber Systems. To ensure this is clear in the Annual Declaration, the language of declaration 7 is revised as follows:

> Contracts with third-party service providers for Critical Cyber Systems include cybersecurity terms and conditions.

For declaration 8, while not all assets support the use of complex or long passwords, especially legacy Operational Technology assets, public utilities are expected to document the user account and password capabilities of their Critical Cyber Systems assets and to configure accounts and strong passwords as per supported asset capability. Therefore, declaration 8 is revised as follows to clarify its intent:

> 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 as per capability.

For declaration 9, the Panel notes that not all cyber assets support installation of malware detection and protection tools. Public utilities are expected to install malware detection and protection tools where supported and where operationally feasible so as to not interfere with critical operational processes, and document exceptions with reasons and compensating measures. Therefore declaration 9 is revised as follows:

> Malware detection and protection tools are installed on Critical Cyber Systems assets where technically and operationally feasible.

The Panel is persuaded by Corix's submission that the due date for the declaration should be changed from two months to four months after the fiscal year-end, to align with the deadline for public utility annual reports. Therefore, the Filing Instructions on the Annual Declaration are revised as:

> This declaration is to be completed by the public utility, as defined in section 1 of the *Utilities Commission Ac*t (UCA) and sent as a separate confidential filing with the annual report.

The Panel is persuaded by Corix's submission that the requirement to read and understand the entire UCA is onerous for the Authorized Signing Officer, and that for the purposes of this declaration, the BCUC amend the declaration to include only the relevant sections of the UCA. The Panel considers instead that an understanding of the Cybersecurity Framework is relevant to the Annual Declaration and therefore the declaration "I have read and understand the *Utilities Commission Act*" is replaced with:

> I have read and understood the Cybersecurity Framework.

The Panel notes FortisBC's suggestion that a process to identify critical cyber assets is necessary for a cybersecurity program. However, the Panel is not persuaded that this should be added to the Annual

Declaration because a critical cyber asset identification process is an implicit and necessary requirement to establish the scope of the cybersecurity program.[33]

The Panel sees merit in BC Hydro and FortisBC's submissions to not require the sharing of confidential cybersecurity information along with the Annual Declaration. The Panel confirms that sharing confidential information with the BCUC may be through meetings and other alternative means that may be identified in future.

The Panel further considers it appropriate to revise instruction (2) to include the following, to allow public utilities to better approximate the progress of their cybersecurity program implementation:

> Include approximate **% Completed** for "Partial" responses.

The Panel sees merit in BC Hydro's submission that instructions (3) and (4) be removed to improve the clarity of the Annual Declaration. Further, instruction (5) has also been removed as the terms are already defined in the Cybersecurity Framework. The Cybersecurity Framework has been revised accordingly.

DATED at the City of Vancouver, in the Province of British Columbia, this 2nd day of June 2023.

Original signed by:

D. M. Morton
Commissioner

[33] Order G-385-22, Appendix B1, pp. 3-4.

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-126-23

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, Commissioner

on June 2, 2023

ORDER

WHEREAS:

A. 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;

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

C. 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;

D. By Order G-385-22, dated December 23, 2022, the BCUC established a comment process regarding a proposed two-year pilot of the Cybersecurity Framework (Pilot) and established a regulatory timetable;

E. The regulatory timetable included an opportunity for public utilities to file letters of comment regarding the establishment of the Pilot, the proposed Cybersecurity Framework, and the proposed annual cybersecurity declaration for public utilities; and

F. The BCUC has reviewed the letters of comment received and considers that the following determinations are warranted.

NOW THEREFORE for the reasons provided in the decision issued concurrently with this order, the BCUC orders the following:

1. The Pilot is established for two calendar years with an effective date of January 1, 2024.

2. The Cybersecurity Framework for Public Utilities Version 1.1A attached as Appendix A to the Decision is adopted as the final cybersecurity framework for the Pilot.

3. The Annual Cybersecurity Declaration for Public Utilities Version 1.1A attached as Appendix B to the Decision is adopted as the final annual declaration for the Pilot.

4. Public utilities must file the Annual Declaration for Public Utilities Version 1.1A, attached as Appendix B to the Decision, as per the filing instructions in the declaration.

5. Public utilities must file progress reports with the BCUC on September 1, 2023, and November 1, 2023, attesting to their plans and preparedness to meet the Pilot effective date of January 1, 2024.

6. In addition to the annual reporting requirements outlined in directive 4, public utilities must also file the Annual Declaration for Public Utilities Version 1.1A on or before January 1, 2024, confirming implementation of the Cybersecurity Framework.

7. All cybersecurity information filed by public utilities with the BCUC will be held confidential as disclosure of such information could be harmful to public safety.

DATED at the City of Vancouver, in the Province of British Columbia, this 2nd day of June 2023.

BY ORDER

Original signed by:

D. M. Morton
Commissioner

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

Cybersecurity Framework for Public Utilities

Version 1.1A

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 Standards and Technology (NIST) Cybersecurity Framework Version 1.1 to be the most suitable framework for adoption in British Columbia (B.C.). 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 in the Cybersecurity Framework and related documentation. Defined terms are used in their capitalized form as defined here.

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.
BES Cyber System	BES Cyber Systems as defined in the NERC Glossary of Terms,[1] are subject to compliance with the MRS in B.C. BES Cyber Systems are excluded from Critical Cyber 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 degraded or compromised, could adversely impact the Service of the public utility. A Critical Cyber Asset may be a physical device or a virtual device, for example, a container, virtual server or virtual firewall. This includes redundant and standby devices.
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. Critical Cyber Systems exclude BES Cyber Systems.
Cybersecurity Information	Non-public information about Critical Cyber Systems and their components that could be misused by an adversary to gain unauthorized access to Critical Cyber Systems, that may adversely impact the Service of the public utility. Cybersecurity information may be physical or electronic and includes but is not limited to cyber asset configurations, user accounts and passwords, physical and electronic access control systems configurations, network

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

Term	Definition
	information, backup and restoration plans, incident response plans, security monitoring information and physical plant layout drawings.
IT	Information Technology, includes computers, network devices, security devices and other equipment used for business processes such as customer management, billing and accounting.
MRS	Mandatory Reliability Standards adopted by the BCUC.
NERC	North American Electric Reliability Corporation.
NIST	National Institute of Standards and Technology.
OT	Operational Technology, includes computers, network devices, process controllers, remote terminal units, measurement devices, sensors and other equipment used to monitor and control operational processes such as power generation and distribution, steam generation and distribution and gas distribution.
Service	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.

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 Critical Cyber Systems. Public utility BES Cyber Systems subject to MRS compliance are excluded. Critical Cyber Systems include IT Critical Cyber Systems and OT Critical Cyber Systems necessary to provide safe and adequate Service. These Critical Cyber Systems may be owned or operated by the public utility, owned or operated by the public utility's parent organization or hosted by third-party infrastructure providers such as cloud service providers.

With respect to Thermal Energy Systems, at this time, the Cybersecurity Framework is applicable to Stream B Thermal Energy Systems only.

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.

5.0 B.C. 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 Version 1.1. 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 Critical Cyber 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 that the public utility has not implemented adequate cybersecurity measures, such that the Service of that public utility is not in all respects safe and adequate then the BCUC may order the public utility to implement specific cybersecurity measures.

The version of the B.C. Cybersecurity Framework will follow the version of the adopted NIST Cybersecurity Framework, with an uppercase letter appended to denote the B.C. release. The initial version of the B.C. Cybersecurity Framework is Version 1.1A. Any subsequent revisions to the B.C. framework, based on the NIST Cybersecurity Framework Version 1.1 will be Version 1.1B, 1.1C, and so on.

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 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.

Review and Reporting

The BCUC requires public utilities to report to the BCUC all cybersecurity incidents as per the following procedure:

a. Initial notification must be provided to the BCUC as soon as practicable by any means specified by the BCUC, for the following:

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

(i) confirmation of a cybersecurity incident that impacted a Critical Cyber System and caused partial or total loss of production, generation, storage, transmission, sale, delivery or provision of any product or commodity in which the public utility is engaged; or
(ii) confirmation of a physical security incident that posed a risk to a Critical Cyber System at a facility.

b. Initial notification must be provided to the BCUC by any means specified by the BCUC, within two business days of the following:
   (i) confirmation of a cybersecurity incident that impacted a Critical Cyber System but did not cause any loss of production, generation, storage, transmission, sale, delivery or provision of any product or commodity in which the public utility is engaged; or
   (ii) confirmation of an attempted physical security incident that posed a risk to a Critical Cyber System at a facility.

c. Initial notification must be provided to the BCUC of cybersecurity incidents or physical security events that could pose a risk to Critical Cyber Systems that are pending confirmation five business days after detection. Further notification must be provided if the incident is confirmed.

Public utilities are expected to include the following minimum information in their incident reports. Information may be added progressively to report updates as it becomes available.

- Date and time of the incident report.
- Date and time the incident was detected.
- Date and time the incident was confirmed.
- Facilities at which the incident occurred.
- Type of incident, whether electronic or physical.
- Critical Cyber Systems impacted.
- Description of the impact on Critical Cyber Systems.
- Physical facilities impacted.
- Description of the impact on physical facilities.
- Non-critical IT or OT systems impacted.
- Description of the impact on non-critical IT or OT systems.
- Extent of degradation or loss of the public utility's Service, if any, including loss of view or loss of control of a process.
- Personal or confidential information exfiltrated.
- Cybersecurity Information exfiltrated.
- Ransom demand, if any.
- Status of each of the following: incident containment, restoration of impacted Service, investigation.
- Provincial and federal agencies informed or engaged in the investigation.
- Additional information obtained since the last report.
- Date and time the incident was declared closed.

The public utility must provide periodic updates at least every month or as otherwise requested by the BCUC until the incident is declared closed. This will be followed by a final closing report to the BCUC within 60 days of the incident being closed.

All cybersecurity incident reports must be clearly marked as being confidential.

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 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 prescribed format. The BCUC may conduct a detailed review of the public utility's cybersecurity program if warranted.

Data Storage, Retention and Security

The BCUC recommends that public utilities secure all information and records pertaining to cybersecurity to ensure they are adequately protected. Cybersecurity program review records, evidence of conformance with the cybersecurity controls and other records are expected to be retained for a minimum of five years. Public utilities are advised to conduct appropriate security assessments prior to transferring or storing their cybersecurity information outside Canada.

Confidentiality

All cybersecurity information submitted by public utilities will be held confidential by the BCUC.

bcuc
British Columbia Utilities Commission

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

CONFIDENTIAL

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 by the public utility, as defined in section 1 of the *Utilities Commission Act* (UCA) and sent as a separate confidential filing with the annual report.		
Applicant Information		
Public Utility Name:	BC Business Registration No.:	
Contact Address:		
Contact Phone:	Contact Email:	
Reporting period:		
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 Critical Cyber System assets where feasible and required to maintain accepted security levels.	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. Contracts with third-party service providers for Critical Cyber Systems include cybersecurity terms and conditions.	Yes No Partial	

Form: ADCSF1.1A, June 2, 2023

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 as per capability.	Yes ○ No ○ Partial ○	
9. Malware detection and protection tools are installed on Critical Cyber Systems assets where technically and operationally feasible.	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 understood the Cybersecurity Framework.

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". Include approximate **% Completed** for "Partial" responses.

Form: ADCSF1.1A, June 2, 2023

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

Cybersecurity Framework for Public Utilities

Version 1.~~0~~1A

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~~Standards and Technology (NIST) Cybersecurity Framework ~~version~~Version 1.1 to be the most suitable framework for adoption in British Columbia (~~BC).~~B.C.). 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~~:~~ in the Cybersecurity Framework and related documentation. Defined terms are used in their capitalized form as defined here.

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~~B.C. BES Cyber Systems are excluded from ~~Applicable~~Critical Cyber 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 degraded or compromised, could adversely impact the Service of the public utility. A Critical Cyber Asset may be a physical device or a virtual device, for example, a container, virtual server or virtual firewall. This includes redundant and standby devices.
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. Critical Cyber Systems exclude BES Cyber Systems.
Cybersecurity Information	Non-public information about Critical Cyber Systems and their components that could be misused by an adversary to gain unauthorized access to Critical Cyber Systems, that may adversely impact the Service of the public utility. Cybersecurity information may be physical

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

Term	Definition
	or electronic and includes but is not limited to cyber asset configurations, user accounts and passwords, physical and electronic access control systems configurations, network information, backup and restoration plans, incident response plans, security monitoring information and physical plant layout drawings.
IT	Information Technology, includes computers, network devices, security devices and other equipment used for business processes such as customer management, billing, and accounting, etc.
MRS	Mandatory Reliability Standards adopted by the BCUC.
NERC	North American Electric Reliability Corporation.
NIST	National Institute of ScienceStandards and Technology.
OT	Operational Technology, includes computers, network devices, process controllers, remote terminal units, measurement devices, sensors and other equipment used to monitor and 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.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.

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 ApplicableCritical Cyber Systems. Public utility BES Cyber Systems subject to MRS compliance are excluded. ApplicableCritical Cyber Systems include Information Technology (IT) Critical Cyber Systems and Operational Technology (OT) Critical Cyber Systems necessary to provide safe and adequate Service. These Critical Cyber Systems may be owned or operated by the public utility, owned or operated by the public utility's parent organization or hosted by third-party infrastructure providers such as cloud service providers.

With respect to Thermal Energy Systems, at this time, the Cybersecurity Framework is applicable to Stream B Thermal Energy Systems only.

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.

5.0 ~~BC~~B.C. 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 Version 1.1. 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~~Critical Cyber 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~~of that public utility is not in all respects safe and adequate then the BCUC may order the public utility to implement specific cybersecurity measures.

The version of the B.C. Cybersecurity Framework will follow the version of the adopted NIST Cybersecurity Framework, with an uppercase letter appended to denote the B.C. release. The initial version of the B.C. Cybersecurity Framework is Version 1.1A. Any subsequent revisions to the B.C. framework, based on the NIST Cybersecurity Framework Version 1.1 will be Version 1.1B, 1.1C, and so on.

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~~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.~~

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

Review and Reporting

The BCUC requires public utilities to report to the BCUC all cybersecurity incidents as per the following procedure:

a. Initial notification must be provided to the BCUC as soon as practicable by any means specified by the BCUC, for the following:
   (i) confirmation of a cybersecurity incident that impacted a Critical Cyber System and caused partial or total loss of production, generation, storage, transmission, sale, delivery or provision of any product or commodity in which the public utility is engaged; or
   (ii) confirmation of a physical security incident that posed a risk to a Critical Cyber System at a facility.

b. Initial notification must be provided to the BCUC by any means specified by the BCUC, within two business days of the following:
   (i) confirmation of a cybersecurity incident that impacted a Critical Cyber System but did not cause any loss of production, generation, storage, transmission, sale, delivery or provision of any product or commodity in which the public utility is engaged; or
   (ii) confirmation of an attempted physical security incident that posed a risk to a Critical Cyber System at a facility.

c. Initial notification must be provided to the BCUC of cybersecurity incidents or physical security events that could pose a risk to Critical Cyber Systems that are pending confirmation five business days after detection. Further notification must be provided if the incident is confirmed.

Public utilities are expected to include the following minimum information in their incident reports. Information may be added progressively to report updates as it becomes available.

- Date and time of the incident report.
- Date and time the incident was detected.
- Date and time the incident was confirmed.
- Facilities at which the incident occurred.
- Type of incident, whether electronic or physical.
- Critical Cyber Systems impacted.
- Description of the impact on Critical Cyber Systems.
- Physical facilities impacted.
- Description of the impact on physical facilities.
- Non-critical IT or OT systems impacted.
- Description of the impact on non-critical IT or OT systems.
- Extent of degradation or loss of the public utility's Service, if any, including loss of view or loss of control of a process.
- Personal or confidential information exfiltrated.
- Cybersecurity Information exfiltrated.
- Ransom demand, if any.
- Status of each of the following: incident containment, restoration of impacted Service, investigation.
- Provincial and federal agencies informed or engaged in the investigation.
- Additional information obtained since the last report.
- Date and time the incident was declared closed.

The public utility must provide periodic updates at least every month or as otherwise requested by the BCUC until the incident is declared closed. This will be followed by a final closing report to the BCUC within 60 days of the incident being closed.

All cybersecurity incident reports must be clearly marked as being confidential.

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 prescribed format ~~shown as Attachment B-2.~~ The BCUC may conduct a detailed review of the public utility's cybersecurity program if warranted.

Data Storage, Retention and Security

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

Confidentiality

~~The confidentiality of all~~All cybersecurity information ~~collected~~submitted by public utilities will be held confidential by the BCUC ~~will be determined in accordance with the BCUC's Rules of Practice and Procedure~~.