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

ORDER NUMBER
G-262-25

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

and

British Columbia Utilities Commission
Cybersecurity Framework for Public Utilities

BEFORE:
B. A. Magnan, Commissioner

on November 5, 2025

ORDER

WHEREAS:

A. By Order G-126-23 dated June 2, 2023, the British Columbia Utilities Commission (BCUC) established a two-year pilot (Pilot) of a cybersecurity framework for public utilities (Cybersecurity Framework), effective January 1, 2024, to help mitigate cybersecurity risks to public utilities;

B. During the Pilot, public utilities were required to implement a cybersecurity program based on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF v1.1), report any cybersecurity incidents impacting, or potentially impacting, the utility's critical cyber systems, and file an annual declaration, reporting on the utility's progress in implementing key cybersecurity functions;

C. Based on the experience with the Cybersecurity Framework throughout the Pilot period, the BCUC proposes to implement the Cybersecurity Framework on a permanent basis subject to revisions, including but not limited to:

- Updating the Cybersecurity Framework to reference the current NIST CSF 2.0 instead of NIST CSF v1.1;
- Eliminating the requirement for public utilities that have no Critical Cyber Systems to file an annual cybersecurity declaration;
- Adding a new defined term for "Cybersecurity Incident", new cybersecurity incident reporting categories, and timeframes for public utilities to implement or update their cybersecurity programs under different scenarios, including a proposed two-year timeframe for transitioning to NIST CSF 2.0; and

D. The BCUC considers that a comment process to consider establishment of the Cybersecurity Framework on a permanent basis is warranted.

NOW THEREFORE the BCUC orders the following:

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

2. Parties are invited to submit letters of comment for the BCUC's consideration on the following:
   i) The establishment of the Cybersecurity Framework on a permanent basis;
   ii) The Cybersecurity Framework for Public Utilities attached as Appendix B to this order;
   iii) The Annual Cybersecurity Declaration for Public Utilities attached as Appendix C to this order; and
   iv) The Cybersecurity Incident Reporting Form for Public Utilities attached as Appendix D 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. Letters of comment must be submitted by way of the Letter of Comment Form on the BCUC's website at https://www.bcuc.com/Forms/LetterOfComment.

DATED at the City of Vancouver, in the Province of British Columbia, this 5th day of November 2025.

BY ORDER

Electronically signed by Bernard Magnan

B. A. Magnan
Commissioner

Attachments

British Columbia Utilities Commission
Cybersecurity Framework for Public Utilities

REGULATORY TIMETABLE

Action	Date (2025)
Letters of comment deadline	Wednesday, November 26

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

DRAFT
Cybersecurity Framework for Public Utilities 2.0A

1.0 BACKGROUND

The British Columbia Utilities Commission (BCUC) has general supervision of 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.

In 2022, the BCUC surveyed commonly adopted cybersecurity standards and frameworks and identified the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) to be the most suitable framework for adoption in British Columbia (B.C.). In the sections below, the BCUC sets out its expectations for the implementation of a cybersecurity framework for public utilities (Cybersecurity Framework) based on the NIST CSF.

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.

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 the definition of 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 Incident	A physical or electronic event that has an impact on, or has the potential to impact, Critical Cyber Assets, Cybersecurity Information or physical facilities hosting Critical Cyber Assets or Cybersecurity Information. Unauthorized access or physical damage may disrupt the public utility's Service or result in the loss of Cybersecurity Information. The event may be an

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

Term	Definition
	outcome of a deliberate or inadvertent action, initiated by external threat agents, employees, contractors or vendors.
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 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 electronic 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 that have Critical Cyber Systems and are actively regulated by the BCUC to implement a cybersecurity program based on the NIST CSF 2.0[2] 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 (TES), the Cybersecurity Framework is applicable to District TES (formerly Stream B TES) only.

4.0 NIST CSF 2.0

The NIST CSF 2.0 includes three key components:

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

b. **CSF Organizational Profiles** are an organization's unique alignment of their organizational requirements and objectives, risk appetite, and resources against the desired outcomes of the CSF Core.

[2] NIST CSF 2.0, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Organizational Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization.

c. **CSF Tiers** assist organizations by providing context on how an organization views cybersecurity risk management. The CSF 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.

5.0 B.C. IMPLEMENTATION APPROACH

Public utilities that have a cybersecurity program using the NIST CSF v1.1 are expected to update their cybersecurity program to the NIST CSF 2.0. Public utilities that have a cybersecurity program based on other standards or frameworks are expected to update their program to map to the NIST CSF 2.0 for their Critical Cyber Systems. Public utilities with Critical Cyber Systems that do not have a cybersecurity program are expected to develop a program based on the NIST CSF 2.0 or other cybersecurity standard or framework and map it to the NIST CSF 2.0.

If a public utility does not implement the NIST CSF 2.0, or if the BCUC has concerns with the adequacy of its cybersecurity 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.

5.1 Establishing a Cybersecurity Program

The BCUC expects public utilities to review the NIST CSF 2.0 and related guidance and implementation examples to establish or update their cybersecurity program. Public utilities may also develop a cybersecurity program based on other cybersecurity standards or frameworks and map it to the NIST CSF 2.0.

A public utility that has determined that it does not have Critical Cyber Systems or Cybersecurity Information is not required to establish a cybersecurity program. However, the utility must still conduct an annual internal review of its systems to confirm and document that it has not acquired new Critical Cyber Systems.

5.2 Review and Reporting

Public utilities are required to report all Cybersecurity Incidents to the BCUC. The Cybersecurity Incident Category reporting requirements are as follows:

a. **Category 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 Service; or
    (ii) confirmation of a physical security incident that posed a risk to a Critical Cyber System at a facility.

b. **Category 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 Service; or
    (ii) confirmation of an attempted physical security incident that posed a risk to a Critical Cyber System at a facility.

c. **Category 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 updates must be provided until the incident is confirmed or closed.

d. **Category D**: Initial notification to the BCUC within five business days of being notified of Cybersecurity Incidents at a partner, affiliate, owner or vendor organization that has authorized access to the public utility's IT or OT systems, and the public utility was notified of the incident by the impacted organization. The incident did not impact the public utility's Critical Cyber System(s) or a facility of the public utility with a Critical Cyber System.

e. **Category E**: Voluntary reporting on other significant cybersecurity issues that the public utility would like to report to the BCUC.

Public utilities are expected to include the following minimum information in their incident reports. Information may be added progressively to incident 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 an industrial 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.
- Date and time the incident was declared closed.

The public utility must provide monthly incident updates from the date of the initial incident report 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. The closing report should include a description of any corrective actions taken and/or preventive actions implemented to improve cybersecurity controls at the utility to prevent recurrence.

All cybersecurity incident reports must be clearly marked as being confidential. Public utilities may use their existing incident report formats or use the Cybersecurity Incident Reporting Form for Public Utilities.

The BCUC expects that each public utility will review its cybersecurity program annually, identify gaps and opportunities for improvement and create a corrective and improvement actions plan, that the utility reviews and updates periodically.

Each public utility must submit an annual cybersecurity declaration to the BCUC in the prescribed format. The annual cybersecurity declaration will be for the preceding fiscal year for the utility and should be filed as a separate confidential filing when the public utility's annual report is filed.

Public utilities that have no Critical Cyber Systems or Cybersecurity Information are not required to file the annual cybersecurity declaration. These public utilities should maintain internal records, reviewed at least annually, confirming they have no Critical Cyber Systems or Cybersecurity Information and be able to provide such records to the BCUC on request. Public utilities are expected to notify the BCUC as soon as practicable and no later than 60 days of any changes in circumstances resulting in the public utility acquiring Critical Cyber Systems or Cybersecurity Information.

The BCUC may conduct a detailed review of the public utility's cybersecurity program and related records if warranted.

5.3 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 and records outside Canada.

5.4 Confidentiality

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

5.5 Implementation Plan

The timeframe for a public utility to complete its development, implementation, migration or mapping to the NIST CSF 2.0 is as follows.

a. **Existing cybersecurity program based on NIST CSF v1.1**
A public utility that has an established cybersecurity program based on the NIST CSF v1.1 is expected to update its program to the NIST CSF 2.0 by December 31, 2027.

b. **Existing cybersecurity program based on NIST CSF 2.0**
There is no further action required by a public utility that has a cybersecurity program that is based on the NIST CSF 2.0 and meets the BCUC Cybersecurity Framework requirements.

c. **Existing non-NIST CSF cybersecurity standard or framework**
A public utility with a cybersecurity program based on a cybersecurity standard or framework other than the NIST CSF is expected to update its program and mapping to meet the requirements of the NIST CSF 2.0 by December 31, 2027.

d. **Existing utility with no cybersecurity program**
A public utility that currently has no Critical Cyber Systems and consequently no cybersecurity program, upgrades its facilities to include Critical Cyber Systems. The utility is expected to have a cybersecurity program based on or mapped to the NIST CSF 2.0 by the commissioning date of the Critical Cyber Systems.

e. **Newly established facilities**
A public utility that is installing new facilities that include potential Critical Cyber Systems to provide Service, is expected to have a cybersecurity program based on or mapped to the NIST CSF 2.0 by the commissioning date of the Critical Cyber Systems.

f. **Newly designated public utility**
An entity that is a newly designated public utility is expected to have a cybersecurity program based on or mapped to the NIST CSF 2.0 within 24 months of the new public utility designation.

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

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. Please respond to all the items in the declaration. Include a brief explanation for “No” or “Partial" responses. Include approximate % Completed for "Partial" responses.		
Public Utility 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 ◯	

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 ◯	
12. Any other information to be reported (optional).		

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:

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

Cybersecurity Incident Reporting Form for Public Utilities

Filing Instructions	
This form may be used by a public utility to file a cybersecurity incident report as required by the Cybersecurity Framework 2.0A adopted by the BCUC. The form must be converted to a PDF and filed confidentially using the BCUC e-filing portal. See form guidance at end for instructions on filling the form. Important: Please do not email this report to the BCUC.	
Public Utility Information	
Public Utility Name:	BC Business Registration No.:
Contact Address:	
Contact Phone:	Contact Email:
Cybersecurity Incident Information	
1. Incident report type (New Incident Report / Incident Update Report / Incident Closing Report)	
2. Incident category (A - E)	
3. Incident title	
4. Date and time of incident report	
5. Date and time incident was detected	
6. Date and time incident was confirmed	
7. Facilities at which the incident occurred	
8. Type of incident (Electronic / Physical)	
9. Critical Cyber Systems impacted	
10. Description of impact on Critical Cyber Systems	
11. Physical facilities impacted	
12. Description of impact on physical facilities	

13. Non-critical IT or OT systems impacted	
14. Description of impact on non-critical IT or OT systems	
15. Extent of degradation or loss of Service	
16. Personal or confidential information exfiltrated	
17. Cybersecurity Information exfiltrated	
18. Ransom demand, if any	
19. Status of incident containment	
20. Status of restoration of impacted Service	
21. Status of investigation	
22. Provincial agencies informed or engaged	
23. Federal agencies informed or engaged	
24. Date and time the incident was declared closed.	
I am authorized to file this incident report on behalf of the public utility. The information set out herein is complete and accurate, to the best of my knowledge, information, and belief.	
Signature of Authorized Signing Officer:	
Name:	
Official Title:	

Cybersecurity incident reporting form guidance

1. Refer to the Cybersecurity Framework 2.0A for definitions of terms, incident categories and other information on cybersecurity incident reporting.
2. Provide as much information as is available when the first incident report is filed. Update or add new information in periodic update reports.

Form Item	Description and Examples
1. Incident report type	This is the type of report to be selected in the BCUC e-filing portal. **New Incident Report**: usually the first report filed for a new incident **Incident Update Report**: typically filed monthly after the New Incident Report, with additional information. **Incident Closing Report**: filed when the incident is declared closed. Note: this is not the final closing report that must be filed no later than 60 days of the incident being closed.
2. Incident category	The Category of the incident, between A and E. Please refer to the Cybersecurity Framework 2.0A for detailed descriptions. **Category A** (i) Confirmation of a Cybersecurity Incident that impacted a Critical Cyber System and caused partial or total loss of Service; or (ii) Confirmation of a physical security incident that posed a risk to a Critical Cyber System at a facility. **Category B** (i) Confirmation of a Cybersecurity Incident that impacted a Critical Cyber System but did not cause any loss of Service; or (ii) Confirmation of an attempted physical security incident that posed a risk to a Critical Cyber System at a facility. **Category C** 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 updates must be provided until the incident is confirmed or closed. **Category D** Cybersecurity Incidents at a partner, affiliate, owner or vendor organization that has authorized access to the public utility's IT or OT systems, and the public utility was notified of the incident by the impacted organization. The incident did not impact the public utility's Critical Cyber System(s) or a facility of the public utility with a Critical Cyber System. **Category E**

	Voluntary reporting on other significant cybersecurity issues that the public utility would like to report to the BCUC.
3. Incident title	A short title, that will also be the "Filing Title" in the BCUC e-filing portal submission. Use the same incident title for all filings related to the incident.
4. Date and time of incident report	The date and time this incident report is created.
5. Date and time incident was detected	The date and time the incident was first detected, either by an automated detection system or by a human operator or analyst. This need not have been confirmed as an incident at this time.
6. Date and time incident was confirmed	The date and time that the incident was confirmed, if different from the date and time the incident was detected.
7. Facilities at which the incident occurred	The names of the locations where there was an impact or potential for impact on the Service. For example, Acme Generating Station or Sky District Energy System.
8. Type of incident	Whether this was an electronic cybersecurity incident or a physical security event.
9. Critical Cyber Systems impacted	The descriptive names of the Critical Cyber Systems that were impacted by the incident; for example, Boiler Management System or Turbine Control System.
10. Description of impact on Critical Cyber Systems	Provide a brief description such as "Malware messages were displayed on operator consoles. The operators activated the incident response plan and informed the IT department. IT consulted with the operations supervisor and isolated the SCADA system to facilitate containment and forensic analysis".
11. Physical facilities impacted	The names of the physical locations where a physical security incident occurred.
12. Description of impact on physical facilities	The impact on the physical facilities; for example, "Suspected vandals forced open the door to the substation that has critical substation automation systems".
13. Non-critical IT or OT systems impacted	Whether any adjacent or unrelated non-critical IT or OT systems were also impacted by this incident. For example, an Internet-facing web server.
14. Description of impact on non-critical IT or OT systems	For example, "A known vulnerability in the public-facing web server was exploited to gain unauthorized access to the IT network. This could have been used to access the SCADA system".
15. Extent of degradation or loss of Service	Estimate the degree of loss or degradation of Service using appropriate metrics; for example, "Steam generation was suspended,

	resulting in loss of thermal energy supply to 200 residential units" or "The substation tripped, resulting in a power outage impacting 2,000 customers".
16. Personal or confidential information exfiltrated	Whether any Personally Identifiable Information was exfiltrated and the number of individuals impacted. For example, "Information comprising the names, emails, phone numbers, residential addresses, account numbers and payment information of 2,000 customers was exfiltrated from the Customer Billing System".
17. Cybersecurity Information exfiltrated	Whether any sensitive information classified as Cybersecurity Information was exfiltrated, and the nature and volume of information. For example, "100 GB of SCADA design, configuration and backup information were exfiltrated".
18. Ransom demand, if any	Yes or no.
19. Status of incident containment	Has the incident been contained as per best information available at the time of this report?
20. Status of restoration of impacted Service	Has the Service been restored partially or completely, if impacted? To what extent has it been restored? For example, "Service to all 2,000 customers was restored within 2 hours and 45 minutes of the beginning of the outage".
21. Status of investigation	For example, "The investigation is ongoing with the help of an external cybersecurity incident response agency".
22. Provincial agencies informed or engaged	Names of provincial agencies informed or engaged.
23. Federal agencies informed or engaged	Names of federal agencies informed or engaged.
24. Date and time the incident was declared closed.	The date and time at which the incident was declared closed by the incident response team lead or by the designated senior manager.

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~~

DRAFT
Cybersecurity Framework for Public Utilities
~~Version 1.1A~~2.0A

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~~In 2022, the BCUC surveyed commonly adopted cybersecurity standards and frameworks and~~, based on its assessment, considers~~ identified the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity ~~Framework Version 1.1~~(NIST CSF) 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~~the implementation of a cybersecurity framework for public utilities ~~will implement~~(Cybersecurity Framework) based on the NIST ~~Framework~~CSF.

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 the definition of 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.

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

Term	Definition
Cybersecurity Incident	A physical or electronic event that has an impact on, or has the potential to impact, Critical Cyber Assets, Cybersecurity Information or physical facilities hosting Critical Cyber Assets or Cybersecurity Information. Unauthorized access or physical damage may disrupt the public utility's Service or result in the loss of Cybersecurity Information. The event may be an outcome of a deliberate or inadvertent action, initiated by external threat agents, employees, contractors or vendors.
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~~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 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 electronic 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 that have Critical Cyber Systems and are actively regulated by the BCUC to implement a cybersecurity program based on the NIST ~~Cybersecurity Framework~~CSF 2.0[2] 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,~~ (TES), the Cybersecurity Framework is applicable to District TES (formerly Stream B ~~Thermal Energy Systems~~TES) only.

4.0 NIST ~~CYBERSECURITY FRAMEWORK~~CSF 2.0

~~**NIST Cybersecurity Framework Overview**~~

The NIST ~~Cybersecurity Framework~~CSF 2.0 includes three key components: ~~(i) the Framework Core; (ii) Framework Implementation Tiers; and (iii) Framework Profiles.~~

[2] NIST CSF 2.0, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

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

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

c. **CSF Tiers** assist organizations by providing context on how an organization views cybersecurity risk management. The ~~Implementation~~CSF 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 using the NIST CSF v1.1 are expected to ~~improve that program or establish a new~~ update their cybersecurity program ~~based on~~to the NIST ~~Cybersecurity Framework Version 1.1~~CSF 2.0. Public utilities that ~~already~~ have a ~~well-established~~ cybersecurity program based on other standards or frameworks ~~may instead~~are expected to update their program to map ~~that program~~ to the NIST ~~Cybersecurity Framework~~CSF 2.0 for their Critical Cyber Systems. Public utilities with Critical Cyber Systems that do not have a cybersecurity program are expected to develop a program based on the NIST CSF 2.0 or other cybersecurity standard or framework and map it to the NIST CSF 2.0.

If a public utility does not implement the NIST ~~Cybersecurity Framework~~CSF 2.0, or if the BCUC has concerns with the adequacy of ~~the~~its cybersecurity 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.~~

5.1 Establishing a Cybersecurity Program

The BCUC expects public utilities to review ~~and follow the seven-step process documented by~~ the NIST ~~Cybersecurity Framework~~CSF 2.0 and related guidance and implementation examples to establish or ~~improve~~update 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[3] for more information on the development and improvement of~~ Public utilities may also develop a cybersecurity program~~. The BCUC may issue implementation guidance from time to time.~~ based on other cybersecurity standards or frameworks and map it to the NIST CSF 2.0.

A public utility that has determined that it does not have Critical Cyber Systems or Cybersecurity Information is not required to establish a cybersecurity program. However, the utility must still conduct an annual internal review of its systems to confirm and document that it has not acquired new Critical Cyber Systems.

5.2 Review and Reporting

~~The BCUC requires public~~Public utilities are required to report all Cybersecurity Incidents to the BCUC ~~all cybersecurity incidents~~. The Cybersecurity Incident Category reporting requirements are as ~~per the following procedure~~follows:

a. **Category 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~~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~~Service; or
   (ii) confirmation of a physical security incident that posed a risk to a Critical Cyber System at a facility.

b. **Category 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~~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~~Service; or
   (ii) confirmation of an attempted physical security incident that posed a risk to a Critical Cyber System at a facility.

c. **Category C**: Initial notification must be provided to the BCUC of ~~cybersecurity incidents~~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~~updates must be provided ~~if~~until the incident is confirmed or closed.

d. **Category D**: Initial notification to the BCUC within five business days of being notified of Cybersecurity Incidents at a partner, affiliate, owner or vendor organization that has authorized access to the public

~~[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf~~

utility's IT or OT systems, and the public utility was notified of the incident by the impacted organization. The incident did not impact the public utility's Critical Cyber System(s) or a facility of the public utility with a Critical Cyber System.

~~c.~~e. **Category E**: Voluntary reporting on other significant cybersecurity issues that the public utility would like to report to the BCUC.

Public utilities are expected to include the following minimum information in their incident reports. Information may be added progressively to ~~report~~incident 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~~an industrial 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~~monthly incident updates ~~at least every month~~from the date of the initial incident report 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. The closing report should include a description of any corrective actions taken and/or preventive actions implemented to improve cybersecurity controls at the utility to prevent recurrence.

All cybersecurity incident reports must be clearly marked as being confidential. Public utilities may use their existing incident report formats or use the Cybersecurity Incident Reporting Form for Public Utilities.

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~~its 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~~, that the utility reviews and updates periodically.

Each public utility must submit an annual cybersecurity declaration to the BCUC in the prescribed format. The annual cybersecurity declaration will be for the preceding fiscal year for the utility and should be filed as a separate confidential filing when the public utility's annual report is filed.

Public utilities that have no Critical Cyber Systems or Cybersecurity Information are not required to file the annual cybersecurity declaration. These public utilities should maintain internal records, reviewed at least annually, confirming they have no Critical Cyber Systems or Cybersecurity Information and be able to provide such records to the BCUC on request. Public utilities are expected to notify the BCUC as soon as practicable and no later than 60 days of any changes in circumstances resulting in the public utility acquiring Critical Cyber Systems or Cybersecurity Information.

The BCUC may conduct a detailed review of the public utility's cybersecurity program and related records if warranted.

5.3 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~~Cybersecurity Information and records outside Canada.

5.4 Confidentiality

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

5.5 Implementation Plan

The timeframe for a public utility to complete its development, implementation, migration or mapping to the NIST CSF 2.0 is as follows.

a. **Existing cybersecurity program based on NIST CSF v1.1**
A public utility that has an established cybersecurity program based on the NIST CSF v1.1 is expected to update its program to the NIST CSF 2.0 by December 31, 2027.

b. **Existing cybersecurity program based on NIST CSF 2.0**
There is no further action required by a public utility that has a cybersecurity program that is based on the NIST CSF 2.0 and meets the BCUC Cybersecurity Framework requirements.

c. **Existing non-NIST CSF cybersecurity standard or framework**
A public utility with a cybersecurity program based on a cybersecurity standard or framework other than the NIST CSF is expected to update its program and mapping to meet the requirements of the NIST CSF 2.0 by December 31, 2027.

d. **Existing utility with no cybersecurity program**
A public utility that currently has no Critical Cyber Systems and consequently no cybersecurity program, upgrades its facilities to include Critical Cyber Systems. The utility is expected to have a cybersecurity program based on or mapped to the NIST CSF 2.0 by the commissioning date of the Critical Cyber Systems.

e. **Newly established facilities**
A public utility that is installing new facilities that include potential Critical Cyber Systems to provide Service, is expected to have a cybersecurity program based on or mapped to the NIST CSF 2.0 by the commissioning date of the Critical Cyber Systems.

f. **Newly designated public utility**

An entity that is a newly designated public utility is expected to have a cybersecurity program based on or mapped to the NIST CSF 2.0 within 24 months of the new public utility designation.