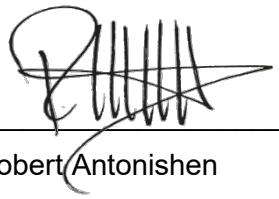
# NERC CIP REQUIREMENTS DIGEST FOR BC HYDRO SUPPLIERS

Approval:



Robert Antonishen
Director, Cybersecurity & Compliance

2024 June 14
Date

Version 2.01, 06/14/2023

## Table of Contents

# Introduction

As required by the North American Electric Reliability Corporation (NERC) reliability standards approved and adopted by the British Columbia Utilities Commission (BCUC), BC Hydro (BCH) is mandated to identify and protect all BCH Critical Infrastructure Protection (CIP) assets which contribute to the safety and reliability of the bulk power system. BCH CIP Assets are classified by "High Impact", "Medium Impact", and "Low Impact" criteria according to their intended functions and afforded the protections required under BCH reliability standard obligations.

# 1. Purpose

This document serves to summarize the guidance and direction for Suppliers doing business with BCH when BCH CIP Assets are involved.

This document describes at a high-level, the relevant BCH CIP controls used when contracting with any third-party Supplier of products or services, to ensure that BCH CIP regulatory compliance obligations are met. These requirements supplement the terms and conditions of any contract or work order into which they are incorporated by reference.

# 2. Scope/Applicability

## 2.1 Scope

BCH CIP Assets are wide-ranging. As required by NERC CIP, there are a variety of controls BCH utilizes to address all "High Impact", "Medium Impact", and "Low Impact" CIP designated classifications.

Please contact the BCH Responsible Manager to inquire whether the scope of work or services performed involve BCH CIP Assets, working in secured areas that contain BCH CIP Assets, or having access to CIP related sensitive information (BCSI).

## 2.2 Applicability

This document applies to all Suppliers that provide products and/or services to BCH which may be subject to regulated compliance requirements as set forth by the NERC CIP Standards.

This document is for use by Suppliers, including consultants and contractors, that have an executed Contract with BCH that involves BCH CIP Assets.

## 2.3 Questions

This document is updated and maintained by the CIP Program Office (CPO). If there are any questions regarding this document itself or issues accessing any information referenced as part of this document, please send in an inquiry to:

- SupplyChain.NERCCIP@bchydro.com

For any other questions regarding NERC CIP as it pertains to your work scope or services provided to BCH, please contact the BCH Responsible Manager.

Note that the NERCCIP mailbox listed above is intended for Suppliers performing work under an executed Contract with BCH. It is not intended for anyone who is currently participating in a procurement process. If you are participating in a procurement process,

you must contact the relevant Procurement Contact Person in accordance with the relevant procurement documentation.

# 3. Acronyms and Definitions

## 3.1 Acronyms

| ACRONYMS | |
|---|---|
| BCSI | Bulk Electric System Cyber System Information |
| BES | Bulk Electric System |
| ERC | External Routable Connectivity |
| IPP | BES Cyber System Information Protection Program (CIP-011) |
| NERC | North American Electric Reliability Corporation |
| N-PSZ | NERC Physical Security Zone |
| N-IPP | NERC Information Protection Program Area |
| PACS | Physical Access Controls Systems |
| PRA | Personnel Risk Assessment |
| PSP | Physical Security Perimeter |

## 3.2 Definitions

| DEFINITIONS | |
|---|---|
| BCH CIP Assets | The term used when referring to assets subject to BCH CIP obligations and their associated:<br>1. BES Cyber Assets (BCAs);<br>2. BES Cyber Systems (BCS);<br>3. Protected Cyber Assets (PCAs);<br>4. Electronic Access Control or Monitoring Systems (EACMS); and<br>5. Physical Access Control Systems (PACS). |
| BCH Responsible Manager | The day-to-day contact and/or work initiator (Hydro's Representative or otherwise as applicable) under the relevant Contract. |
| (BES) Bulk Electric System | "Unless modified by the lists shown below, all Transmission Elements operated at 100 kV or higher"; for simplicity, consider this to be the select facilities in the Transmission and Generation system. |

| | |
|---|---|
| | *Note: This term has been simplified from the official NERC defined term for the purpose of this document, see NERC Glossary for reference: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf* |
| BES Cyber System Information (BCSI) | The terms BES Cyber System Information, BCSI, NERC CIP Confidential Information or CIP Confidential Information (used interchangeably at BCH) refer to information concerning NERC CIP Cyber Assets that:<br>1. Relates to the production, generation or transmission of energy and their related protective systems.<br>2. Could be useful to a person planning an attack on critical infrastructure; and<br>3. Information that is identified as CIP Confidential Information by BCH.<br>These terms mean information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.<br><br>Examples of BCSI include but are not limited to:<br>1. Network diagrams, floor plans, and design plans<br>2. Device configurations, assets lists and reports<br>3. Operational procedures, disaster recovery plans and incident response plans<br>4. Information which has been identified as CIP Confidential by BC Hydro |
| Contract | A standalone agreement or a work authorization issued under a Master Services Agreement. |
| Cyber Security Incident | A malicious act or suspicious event that:<br>For a high or medium impact BES Cyber System, compromises or attempts to compromise<br>1. An Electronic Security Perimeter,<br>2. A Physical Security Perimeter, or<br>3. An Electronic Access Control or Monitoring System; or<br>4. Disrupts or attempts to disrupt the operation of a BES Cyber System. |
| Individual | Any individual performing work under the Supplier's Contract, including employees of the Supplier or its Sub-Contractors. |
| NERC Electronic Access | Remote or local interactive user access to BCH CIP assets that contain External Routable Connectivity (ERC) and local system access to BCH CIP assets without ERC. |
| Removable Media | Storage media that i) are not Cyber Assets, (ii) are capable of transferring executable code, (iii) can be used to store, copy, move, or access data, and (iv) are directly connected for 30 consecutive calendar days or less to a BES Cyber Asset, a network within an ESP, or a Protected Cyber Asset. Examples include, but are not limited to, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory. |

| | |
|---|---|
| Security Command Centre (SCC) | SCC is a staffed centralized function at BC Hydro that operates twenty-four hours per day, seven days a week, which acts as a single point of contact by phone and email for all employees and suppliers on any matters related to physical security. |
| Sub-Contractor | Entity (including any sole proprietor) that the Supplier has contracted with to perform some of the contracted work. |
| Supplier | The entity (including any sole proprietor) that BCH contracts with to provide products and/or perform services. |
| Transient Cyber Asset | A Cyber Asset device that is:<br>1. Capable of transmitting or transferring executable code,<br>2. Not included in a BES Cyber System<br>3. Directly connected to a BCH CIP Asset.<br>Example: Laptops used to perform maintenance work on CIP cyber assets.<br>*Note: This term has been simplified from the official NERC defined term for the purpose of this document, see NERC Glossary for reference: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf* |
| Unescorted Physical Access Requirements | Requirements for gaining unescorted physical access to BCH areas rated as CIP "High Impact" and "Medium Impact". |

# 4. Access

## 4.1 Access Types

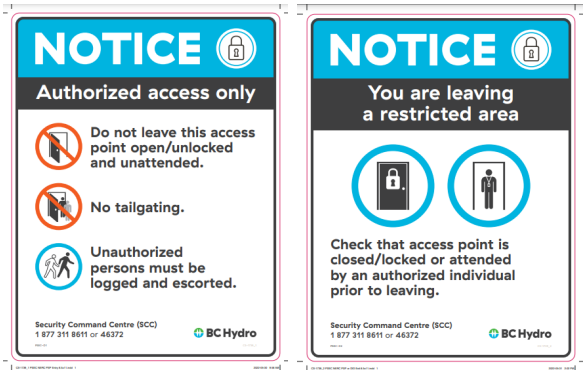
Access to BCH CIP Assets must be need-based and authorized by BCH designated personnel. Access may be obtained physically, electronically, or through received or observed information. This section summarizes the various types of access for Individuals who will work with BCH CIP Assets or BCSI.

## 4.2 CIP Access Zones

BCH classifies areas containing NERC physical BCH CIP Assets into three different restricted areas, the PSP, N-PSZ or N-IPP. All areas require authorization and approval to physically access. Unescorted physical access authorization to these areas is based upon need as required by NERC CIP obligations.

## 4.3 Physical Access[1]

NERC physical access areas are labelled with signage. All entry and exit requirements must be followed by Individuals who possess authorized unescorted Physical Access, or escorted Visitor Access.




Unescorted Physical Access

NERC CIP standards require controls and protections for unescorted physical access at NERC facilities containing BCH CIP Assets which include:

- Requiring Individuals to meet the minimum requirements to be authorized for unescorted physical access to NERC facilities;
- Meeting the minimum requirements to maintain unescorted physical access to NERC facilities; and
- When physical access is no longer necessary, the supplier must notify the BCH Responsible Manager as soon as possible so that revocation of access may occur within the 24-hour requirement mandated under the NERC CIP requirements.

Visitor Access[2]

Visitor Access applies to Individuals who have not received authorization for unescorted physical access to areas containing BCH CIP Assets but still require access to those areas.

All Individuals who do not possess unescorted physical access permissions to PSPs, N-PSZs or N-IPPs shall be classified as Visitors and adhere to established Visitor access controls. Such controls include but are not limited to:

- Visitors are required to complete, in full, the PSP Visitor Log upon arrival and departure from the PSP or PSP-like area upon entry and exit of the area.
- Visitors are required to be issued a physical security badge and to visibly display it at all times during the visit. Example:

- Visitors must be escorted at-all-times by individuals who are authorized for unescorted physical access while inside the designated area and ensure they maintain close proximity and visual contact with their host.
- Visitors are not allowed to physically touch any BCH CIP Assets even under escort.
- No photography or video recording is permitted.
- No Weapons are allowed.
- No threats or acts of violence will be tolerated.
- BCH reserves the right to inspect all packages and personal items.
- In case of an emergency Visitors must follow instructions of the authorized host.
- To obtain, if required, a copy of Chapter 12 - Visitor Hosting and Visitor Pass Management of BC Hydro's Master Physical Security Program coordinate with your authorized host, or email:
    - Physical.Security.NERC.CIP.MRS@bchydro.com

### 4.4 Electronic Access[3]

BCH must afford controls and protections for Individuals who are authorized to receive electronic access to BCH CIP Assets. This section summarizes the controls for electronic access.

Electronic Access Types

- Electronic access is classified by two types:
    - Electronic Access to BCH CIP Assets with External Routable Connectivity (ERC)
    - Electronic Access to BCH CIP Assets without External Routable Connectivity (ERC)

Approval of Access

- Electronic Access to BCH CIP Assets with ERC is authorized through SureSite.

Electronic Access Security Protocols

- Individuals must meet the minimum requirements to be authorized for electronic access to applicable BCH CIP Assets.
- Individuals must meet the minimum requirements to maintain electronic access to applicable BCH CIP Assets.
- When electronic access is no longer necessary, the supplier must notify the BCH Responsible Manager as soon as possible so that revocation of access may occur within the 24-hour requirement mandated under the NERC CIP requirements.

### 4.5 Access to BES Cyber System Information (BCSI)[4]

NERC CIP Confidential information whether physical, electronic, or verbal is protected by BC Hydro's ***BES Cyber System Information Protection Program (IPP)***[a], which is summarized in the Info Sheet on CIP Confidential Information (BCSI). Sensitive information involving BCH CIP Assets is classified as BCSI and is afforded controls and protection as required by the NERC CIP standards.

Individuals are responsible for the protection of BCSI while in use, transit, and storage as it pertains to their work assignment; and to minimize incidental access to the information via visual or verbal disclosure.

Controls apply for the handling, transmittal, storage, and development of any sensitive information involving BCH CIP Assets. Such information may include but is not limited to:

- Network diagrams, floor plans and design plans
- BCH CIP Asset device configurations, asset lists and reports
- Operational procedures, disaster recovery plans and incident response plans
- Information which has been identified as BCSI by BCH

Individuals are to direct questions relating to whether or not a particular type of information or data is BCSI to the BCH Responsible Manager for guidance.

Individuals must confirm in writing to the BCH Responsible Manager their review and understanding of the *Info Sheet on CIP Confidential Information (BCSI).*

### 4.6 Provisioning and Revocation of Access

Provisioning of Access

Individuals who have been authorized for unescorted physical access to areas containing BCH CIP Assets will be issued ID Access Cards and additionally may be issued physical key/electronic access when approved.

All Individuals who are issued these materials must protect and secure these items from loss or theft.

Individuals must report Lost or Stolen Physical Access Cards/ID Cards, keys or electronic passcodes to the Security Command Centre (SCC) at 1-877-311-8611 as soon as possible.

Revocation of Access

- Revocation of access activities described below are regardless of the separation reason (termination, job transfers or reassignments, need-based access no longer needed, etc.)
- Suppliers must ensure that they have a proper off boarding process in place when the Individual's access is no longer necessary or when the Individual separates

[a] Contact the BCH Responsible Manager if a copy of the IPP is required.

from service to allow BC Hydro to revoke the Individual's access within 24 hours as required under NERC CIP obligations. Such processes must include at a minimum:

- A process to notify BC Hydro to revoke the Individual's access within 24 hours when access is no longer needed as required under NERC CIP obligations.
- A process to return the issued BC Hydro Physical Access/ID Card before the Individual's final separation date.
- A process to inform the BCH Responsible Manager immediately to initiate the removal of NERC Electronic Access before the Individual's final separation date.
- A process to return all BC Hydro assets as applicable; (e.g. BC Hydro devices, keys and equipment) before the Individual's final separation date.
- A process to return or certify the destruction of BCSI information in the Individual's possession.

# 5. Obtaining Physical and Electronic Access

## 5.1 Completing Personnel Risk Assessments (PRAs)

Individuals who will need unescorted physical or electronic access to BCH CIP areas must receive a Personnel Risk Assessment at least once every seven (7) calendar years. The PRA includes:

- Confirmation of identity.
- Performance of a seven-year criminal history records check which includes the individual's current residence, regardless of duration, and other locations where during the seven years immediately prior to the date of the criminal history records check, the individual has resided for six consecutive months or more.
- Evaluation of the criminal history records checks used for authorizing access.

## 5.2 Completing Required Training[5]

At a minimum, required Cybersecurity Awareness 101 training shall be completed by Individuals in connection with the executed agreement.

Suppliers shall be required to complete additional CIP related training appropriate to the individual's roles, functions, or responsibilities assigned under the agreement.

Suppliers must ensure that they have a process to ensure that all Individuals complete required NERC CIP Training. Training is completed electronically using the Udutu application.

Individuals shall submit evidence of completing required NERC CIP Training to the BCH Responsible Manager.

Training Frequency

Individuals shall complete all required training at the initial onset of the contract execution, and annually thereafter.

Individuals shall be subject to receiving quarterly Cyber Security Awareness reinforcements from BCH which may be in the form of physical posters, handouts or emails, and may include associated physical security practices.

### 5.3 Pre-Requisite(s) Matrices for CIP Related Access

| Access Type | Requirements |
|---|---|
| Authorized, unescorted physical access to Critical Infrastructure Protection (CIP) assets<br>or<br>Authorized network access to a CIP location, asset, system, or application | 1. Have a valid BC Hydro ID access card.<br>2. Complete the CIP-100, "CIP (Confidential Infrastructure Protection) Awareness" course *annually*.<br>3. Complete a Personnel Risk Assessment (PRA) every 7 years. |
| Escorted or accompanied physical access to Critical Infrastructure Protection (CIP) assets | • Arrangements must be made for the individual to be accompanied by someone with BC Hydro authorized, unescorted physical access |
| Access to CIP Confidential Info (also referred to as "BCSI") | • Complete at least one of the following:<br>○ COPOL 101 – Cybersecurity Awareness101 training<br>○ CIP-100 CIP Awareness training<br>○ Review Info Sheet on CIP Confidential Information (BCSI) |

| **Access Control Process for BCSI Storage Locations** | |
|---|---|
| When BCH owned and managed BCSI Storage Location is used: | When the supplier owned and managed BCSI Storage Location is used: |
| • Follow the BCH Access Authorization Process to obtain approval of use; and<br>• Follow the specific repository provisioning process to receive access. | • Follow supplier's information access authorization and provisioning process.*<br>• Implementation of the process shall produce auditable records of authorization and provisions which shall be provided to the BCH Responsible Manager. |

* When the supplier owned and managed BCSI storage location is used, the supplier's information access authorization and provisioning process for BCSI access must include protection measures for handling, transit and storage of BCSI. Examples of protecting BCSI electronically may include data masking, encryption, hashing, tokenization, cipher, or electronic key management or physical protection lock and key management. Physical protections for the storage of BCSI at the supplier location(s) must also be

addressed.

### 5.4 Requesting Access

Depending on the access required, once pre-requisites are completed, tracked and authorized; the Individual may submit a CIP Access Request via SureSite. Note, the NERC CIP Access workflow will not start without documented evidence of all pre-requisites being satisfied. The BCH Responsible Manager may contact the Individual if there are any outstanding issues that need to be addressed.

Generally, completion of first tier and second tier approvals may take up to a few business days. To avoid any unnecessary delays, Individuals are encouraged to start the NERC CIP Access request process as soon as possible when all completed documentation has been submitted.

Upon submittal of the NERC CIP Access request by the requesting Individual, the Individual should contact the BCH Responsible Manager and notify them that their access request is pending the BCH Responsible Manager's approval. If the Individual is unsure who the BCH Responsible Manager is, they may request the information from Hydro's Representative.

The BCH Responsible Manager is responsible for providing the first-tier approvals for the Individual's requested access.

When the first-tier approval has been authorized, the workflow will progress and be sent to the system owner for second-tier approvals.

## 6. Configuration Change Management[6]

### 6.1 Changes to BCH CIP Assets

All changes to BCH CIP Assets require an independent NERC CIP Change request and are in addition to any other enterprise level or business unit change request processes that may be in place for the work being performed.

All changes to existing baseline configurations must be properly authorized and documented prior to the change taking place.

Suppliers must ensure that all Individuals communicate with the BCH Responsible Manager to ensure that the NERC CIP Change Request has been completed appropriately and authorized.

Suppliers and Individuals should contact the BCH Responsible Manager to inquire about specific roles and work actions as it relates to the NERC CIP Change Request.

## 7. Removal, Disposal, and Replacement of a BCH CIP Asset[7]

### 7.1 Change Management Protocols

Any removal, disposal and replacement of a Cyber Asset is classified as a configuration change and must follow the Section 6 Configuration Change Management protocols.

In cases of any uncertainty in the process below, contact the BCH Responsible Manager for information.

Shipment for Repair

BCH may send CIP Assets containing sensitive information to service provider for diagnose, repair and possibly disposal if repair is not possible.

When the CIP Cyber Asset or its data storage media containing BCSI is not sanitized or encrypted prior to disposal or shipping, chain of custody documentation must be maintained and provided to BC Hydro.

Upon notification ("Request for Quote", or "Return Material Authorization" – RMA) of such a shipment or return for repair, supplier shall provide a reference so that the received sensitive asset is treated properly in accordance with supplier's procedure. BC Hydro may seek to review this procedure for assurance. BCH may choose to not proceed with shipment if the procedures do not meet our sensitive material handling needs.

Receiving

At receiving, the supplier shall receive the package, which is intentionally generic, with proper chain of custody methods. The sensitive package, as identified by RMA# or similar, must be stored in a secure location where only the custodian or their authorized personnel have access to.

Repair

Repair will take place as needed. The repaired device should be wiped of sensitive information, so the return shipment can be treated with normal shipping procedures.

**Evidence**: Proof or statement of sanitization is required. This must be sent to the BCH Responsible Manager for acceptance before the device is treated as a non-sensitive item.

If disposal is required

For a BCH CIP Asset to be disposed by a BCH approved service provider, best efforts shall be taken to ensure that the data storage media is sanitized or encrypted prior to disposal.

Any of the methods to clear, purge, or destroy storage media as described per National Institute of Standards and Technology NIST SP 800-88 Rev 1 Table 5.1 Sanitization Methods.

When it is not possible to sanitize the data storage media prior to disposal, a method such as physical destruction (i.e. drilling holes into the storage media, utilizing an industrial shredder/crusher, incinerating the storage media, etc) or degaussing/magnetic erasure as specified by BCH shall be used in a safe manner.

**Evidence**: Proof or statement of disposal is required. This must be sent to the BCH Responsible Manager for acceptance before the disposed device is treated as a non-sensitive item.

Tracking of the BCH CIP Asset's physical location must continue until the media sanitization, data encryption, or destruction of the data storage media is completed. Also, evidence to demonstrate the disposal of the BCH CIP Asset must be retained and provided to the BCH Responsible Manager.

# 8. Transient Cyber Asset (TCA) and Removable Media (RM) Use on BCH CIP Assets[8]

Established controls are in place for Transient Cyber Assets and Removable Media that are used on BCH CIP Assets to mitigate the risk of malware propagation to BCH's CIP environment. These controls are summarized in this section.

## 8.1 BCH TCA and RM Definitions as it pertains to this document

It is important to note that while the definitions of TCA and RM are specific NERC defined terms as defined in the definitions section of this document, BCH has slightly modified these definitions in section 3.2 for assisting the reader of this document in understanding the TCA and RM terms as they relate to this document's purpose. The definitions are as follows:

- TCAs are programmable devices that make a direct data connection (via Ethernet, serial, USB, or wireless - including Bluetooth or near field communication)to BCH CIP Assets for 30 consecutive days or less.
- RM are storage media devices used to store, copy, move, or access data and are directly connected (via serial, USB) to a BCH CIP Asset for 30 consecutive days or less.

## 8.2 TCA and RM Use Training

All Individuals performing work for more than two weeks on a recurring basis involving TCA or RM use must:

- Have the appropriate NERC access and work authorizations, as described in the preceding sections of this document and possess valid BCH access credentials.
- Complete BCH Green User Training.
- Obtain authorization from BCH to become a Green User.

The BCH Responsible Manager can assist the Individual with determining the need for Green User Training by reviewing the Authorized Devices Scope Job Aid.

Any other Individuals must be escorted by an authorized Green User while performing work.

## 8.3 TCA and RM Use Request and Authorization[9]

All TCA and RM use must be requested from the BCH Responsible Manager and be authorized by BCH authorizing officials.

Upon completion of required training, the BCH Responsible Manager will book a Green Laptop for the Individual to use. The Individual will receive a booking confirmation via email with further instructions.

The Individual shall review the Green Laptop specifications with the BCH Responsible Manager to ensure it is appropriate for the work to be performed on the BCH CIP Asset. Note – Additional software may be installed on the Green Laptop if necessary.

For TCAs, by default, when approved, Individuals shall use TCAs issued to the Individual by BCH – Green Laptops and Legacy TCA devices.

Non-BCH TCAs are generally not allowed to be used for connections to BCH CIP Assets unless it has been authorized for use by BCH under a CIP Exceptional Circumstance condition. Individuals must check with the BCH Responsible Manager to determine if this condition would apply.

In the rare case, the Individual is unable to use the Green Laptop, the Individual must get their own laptop authorized by the BCH Responsible Manager. The Individual shall obtain and complete the Vendor TCA Authorization form[b] from Security NERC Extranet or from the BCH Responsible Manager, and return it to the BCH Responsible Manager.

The Individual completes one form for every TCA device (including any Virtual Machines) that will be used, confirming the device meets the security requirements and is free of malware, per criteria defined in the form.

BC Hydro assesses the provided content and approves or rejects the Vendor TCA Authorization form.

- If rejected – the Individual must address the security gaps on their laptop to get it authorized or use the BCH Green Laptop to perform work.
- If approved – the TCA Authorization is valid until the end of calendar quarter.
- Individual continues to keep the TCA protected for the duration of work, per the completed and approved TCA Authorization form.
- Individual renews authorization, if required, by submitting another request for TCA Authorization Form for approval 30 days before the authorization expiration date.

Before commencing work, the Individual is required to verify their TCA and RM compliance to their BCH Responsible Manager for any on-site work.

If using a **non-BCH TCA**, the Individual must show a current, approved Vendor TCA Authorization for each TCA being used. The Individual will not be able to use the TCA if they do not have it.

Generally RM is discouraged and may only be allowed if other data sharing/storage options are not possible. All RM use must be authorized by BCH prior to use. If RM is necessary:

The only RM that can be used for connections to BCH CIP Assets is the BCH Green RM.

Green RM must be authorized via a dedicated SharePoint request for each work order or equivalent work assignment, prior to connection to field equipment.

Non-BCH RM is not allowed for connections to BCH CIP Assets.

If RM will be connecting to BCH CIP Assets:

- The Individual must use a BCH Green RM device and scan it with a BCH laptop, capture the scan evidence and receive authorization from BCH to use it.

[b] Vendor TCA Authorization Form naming convention is retained in this document.

- RM must be re-scanned as described in the Key Rules for Using TCAs and RM section below.

### 8.4 Additional TCA and RM controls required at the end of each working shift

Individual completes work with TCA or RM and disconnects it from the BCH CIP Asset(s) at the end of the shift.

Whether using a BCH or non-BCH TCA, or Green RM, if the device needs to remain connected to field equipment past the end of the shift, the supplier must inform their BC Hydro Responsible Manager to log the necessary details.

Individual disconnects TCA or RM within 30 days from the initial connection date. The Individual confirms disconnection to their BC Hydro Responsible Manager who will update the log.

### 8.5 Key Rules for Using TCAs and RM

The table below provides a quick overview of rules that the Individual should follow while using TCAs and RM.

| Do… | Don't… |
|---|---|
| **Ensure you are authorized** before connecting any laptops or RM to field equipment:<br>• You are on the **Green Users List**<br>• You have necessary NERC access and work authorizations | • Connect to BCH CIP Assets unless **you** have all required authorizations |
| Validate the **device is authorized** **before** connecting to any BCH CIP Assets:<br><br>• **BCH Laptop:**<br>  • **Green Laptop** or **Legacy TCA** in **BCH TCA Inventory** (additional authorization required to connect to **High Impact** assets)<br>  • **Virtual Machine (VM)** is **official** hardened release, on an authorized laptop<br><br>• **Vendor Laptop:**<br>  • has a **valid Authorization** (additional authorization required to connect to **High Impact** assets)<br>  • **If renewal** is needed, re-submit the form for authorization 30 days before the **expiry date**<br>  • Keep the malware protections on authorized TCAs **up to date at all times**.<br><br>• **Green Removable Media (RM) ONLY:** | • Connect **any unauthorized** devices to field equipment<br><br>• Create a **VM from scratch** or other sources and install on the BC Hydro laptop<br><br>• Connect non-BC Hydro TCAs unless you have a valid Vendor TCA authorization.<br><br>• Use **non-Green RM** with field equipment |

| Do… | Don't… |
|---|---|
| • with green tag or with green label | |
| **Prevent bridging networks:**<br>• **Disconnect** the laptop from **any other network BEFORE** connecting to BCH CIP Asset<br>• Turn **wifi off** if not needed at stations | • Connect the Green Laptop or VMs to the **Internet**<br>• Connect the Green Laptop to **public networks** or **smartphone wifi hotspots** |
| **Disconnect** any device (laptops, RM) from BCH CIP Assets at the **end of the shift**. If it must be left connected:<br>• Inform your BC Hydro on-site contact to **log it** in SharePoint (RTS team), or in CROW (everyone else). | • Leave **devices connected** unnecessarily |
| **Removable Media controls:**<br>• Use **laptops connected directly to BCH CIP Assets** or **shared network drives** for file transfers, instead of RM, if possible<br>• Get Use RM authorization BEFORE you connect any RM to field equipment at selected sites and additional sites<br>  • Do a **full anti-virus scan** of the RM using a BCH Laptop<br>  • Attach the **screenshot** to your request as evidence<br>  • **Repeat** the scan and evidence submission if:<br>  • Connecting RM from a **non-NERC to a NERC** asset in the same facility<br>  • Connecting RM to any asset at a **different facility**<br>  • Connecting RM, that was **left unattended** since the last scan, to any asset<br>• If any **malware** is detected:<br>  • **Stop** using the laptop and RM<br>  • **Call** IT Helpdesk immediately<br>• Ensure that laptops are **not connected to BCH CIP Assets when scanning**<br>• **Reformat the USB Drive** at the end of the job (except back-up USBs) | • **Use RM** if you can use **alternative methods**<br>• Connect **any RM** to **BCH CIP Assets** at the **listed sites** unless you have an **authorized** Use RM Request<br>• Forget to attach the **scan evidence** to your Use RM Request<br>• Continue using devices or fail to notify IT Helpdesk after detecting **malware**<br>• Reformat **BCH USB Drives kept at the facility** for backups |
| **Security reminders:**<br>• **Lock the laptop screen** if you leave it unattended | • Disable **BitLocker**<br>• Modify **security controls**<br>• Leave laptops **unlocked** or in **vehicles** |

| Do… | Don't… |
|---|---|
| • **Physically lock devices** if unattended for longer time<br>• **Connect** the laptop to corporate network and **restart regularly** (weekly) | |

# 9. Cybersecurity Supply Chain Risk Management Practices

The below content of this Section 9 forms part of any Contract incorporating this document only if that Contract:

A. involves cybersecurity services, cyber assets or services related to those cyber assets, and

B. does not reference the "BC Hydro CIP-013 Addendum for Contractors"[c] (the "CIP-013 Addendum").

## 9.1 Supplier (Vendor) Cybersecurity Risk Management Requirements[10]

Suppliers who will be involved in providing potential CIP Cyber Asset products (generally, programmable electronic devices) or services to the bulk electric system may be subject to undergo ongoing Vendor Cyber Security Risk ("**VCRA**") assessments.

These assessments may be performed by a BC Hydro appointed third-party. All such parties have agreements with BC Hydro where there are confidentiality agreements in place. Additional non-disclosure agreements are not required.

Suppliers must support assessments, which include, but are not limited to:

- Review of Supplier cybersecurity policy
- Cyber risk assessment of the Supplier by BCH, or its delegates.
  - These assessments are subject to expiry every 18 months. Timing of which may be sooner or later at BCH discretion; some examples are material business changes (commercial or legal), priorities, scheduling, and previous risk level from previous VCRA, but not limited to these.[11]

## 9.2 Suppliers' duty to mitigate

Suppliers are expected to mitigate cybersecurity risks proactively and reactively in support of BCH's cybersecurity requirements. Such mitigation includes:

- Proactive Mitigation: BCH requires Suppliers to take proactive mitigating measures against cybersecurity events, vulnerabilities or incidents that are known or ought to be known by Suppliers. Suppliers shall also proactively inform BCH when access is no longer required (e.g., due to staff changes, completion of scope of work, etc.).

[c] https://www.bchydro.com/content/dam/BCHydro/customer-portal/documents/corporate/suppliers/cybersecurity-CIP-013-contractor-addendum.pdf

- Reactive Mitigation: In the event BCH is found to be non-compliant against any CIP requirements, and where Supplier(s) are found to be associated with the deficiency, BCH will require participation by the Supplier(s) to develop the necessary mitigation plans to correct the deficiency.

### 9.3 CIP-013 Specific Requirements

BCH has specific NERC obligations to comply with the NERC CIP-013 Supply Chain Risk Management Reliability Standard. In addition to the general supply chain requirements identified in this section, the Supplier must be prepared to perform additional activities, listed below. The titles of the following subsections reflect CIP-013 wording.

Subsections (i) to (iv) are notification and coordination requirements for Suppliers upon findings which are only available to suppliers themselves.

Subsections (v) and (vi) are additional requirements which are sustainment and hence preventative in nature for Suppliers to implement where practical.

#### i. Providing notification of vendor identified incidents[12]

The Supplier must notify Hydro's Representative as named on the Contract, when the products or services provided by the supplier to BCH are identified as posing a cyber security risk to BCH. Information in the notification shall include at a minimum the following:

- Date of initial identification
- Identification of the product and/or services affected
- Identification of the mitigating actions to respond to the identified risk
- Plan of updates (communication schedule) on the progress of described mitigation activities

For example: these are typically information contained in industry practices such as "Technical Bulletins", or "Service Bulletins".

Additionally, the Supplier must notify Hydro's Representative regarding any material business changes, such as mergers and acquisitions.

#### ii. Coordination and performing response activities[13]

The Supplier shall coordinate responses to supplier-identified incidents related to products or services provided by the supplier to BCH that pose cyber security risk to BCH.

Contact Hydro's Representative when required as proactively determined by the Supplier, or reactively when requested by BCH:

- The Supplier submits a plan to BCH to address identified incidents within 30 days of the initial identification.

BCH may require supplier to propose response actions in coordination with BCH, and/or propose a response action plan and schedule acceptable to BCH.

#### iii. Providing notification to revoke remote or on-site access[14]

The Supplier must notify the BCH Responsible Manager when remote or on-site access for Individuals is no longer needed in sufficient time for BCH to terminate access (the practical expectation is within 24 hours of Supplier's awareness).[15] [16]

### iv. Disclosing known vulnerabilities[17]

The Supplier must notify Hydro's Representative as named on the Contract to provide disclosure and remediation to BCH of known or newly found vulnerabilities related to provided products or services.

- Use the same notification activities as in subsection (i).

### v. Providing method to verify software integrity and authenticity[18]

The Supplier must indicate methods to verify software integrity and authenticity of all software (firmware and patches) used on BCH CIP Assets. This applies to initial delivery, and incremental update methods.

Methods for integrity and authenticity check should be indicated through self-apparent instructions or otherwise told to a BCH Responsible Manager.

Depending on the nature of products and services, both descriptions 1 & 2 may apply.

1. For publishers of software (patches and firmware), Suppliers will provide:
   - A list of any additionally associated Original Equipment Manufacturers or publishers (OEM), stating the association.
   - Where practical, state methods and tools used to support the verification and confirm software integrity.
     - State the preferred methods to verify (automated, manual, or none)
     - State the tools provided to BCH to verify (such as cryptographic hash function, other or none)
     - Keep BCH informed when new capabilities become available to the market
     - It is a compliance concern if BCH is not made aware of new capabilities made available to others
   - While expectations continue to change, BCH expects progress and to be kept proactively informed.
2. For Suppliers who use software developed by other parties, the supplier will:
   - Provide a software Bill of Materials (SBOM) where practical (see emerging practices about SBOM here), listing all the open source and third-party components present in a codebase.
   - BCH expects progress and best practices to evolve and to be kept proactively informed.

### vi. Providing coordination of controls[19]

Supplier's own control of access to BCH's system is not sufficient. The supplier must coordinate with the BCH Responsible Manager for:

- Supplier-initiated (human) interactive remote access.

- System-to-system (automated or scheduled) remote access between supplier and BCH systems.

## 10. Version History

| Version | Revision Date | Author(s) | Reviewer(s) | Approver(s) (Sign-off Date) | Description of Change |
|---|---|---|---|---|---|
| V1.0 | 2019-07-17 | Benjamin Ma | n/a | n/a | First initial version of the Vendor Digest document completed and reviewed by all CIP Functional Areas and Legal Team. |
| V1.2 | 2019-09-23 | Kelly Stich | n/a | n/a | Added Configuration Change Management |
| V1.3 | 2019-10-15 | Tracy Betel<br>Dragana Vojakovic | n/a | n/a | Updated **Transient Cyber Assets (TCA) and Removable Media (RM) Protection** section |
| V1.4 | 2020-01-14 | Benjamin Ma | n/a | n/a | Updated the document to account for Access Management corporate program updates and for remediation evidencing. |
| V1.5 | 2020-08-20 | Christine Leung | n/a | n/a | Updated **Section 4.3** Process on the pre-requisites that vendors must have before any work commences and the BCSI storage location access control process. |
| V1.6 | 2021-03-17 | Christine Leung | Mark Christianson<br>Peter Kobzar<br>Shaheen Rehmat<br>Eva Weclaw<br>Yingzi Zhang | | • Section 4.2 Scope – updated wording to provide supporting information to GC 4.25 Electronic Data Site<br>• Section 7.2 Completing NERC CIP Training & PRA – added footnote to bullet 2 for clarity to CLRA contractors<br>• Section 8.3 Weekly Vendor Revocation Verification – added new section to provide information on the weekly vendor revocation verification process<br>• Section 10 Removal, Disposal and Replacement of a Cyber |

| Version | Revision Date | Author(s) | Reviewer(s) | Approver(s) (Sign-off Date) | Description of Change |
|---|---|---|---|---|---|
| | | | | | Asset – added new section to provide supporting information to GC 4.8 Removal, Disposal and Replacement of BC Hydro's Existing Facilities and Property |
| V1.7 | 2021-08-12 | Dragana Vojakovic<br>Tracy Betel | | | Updated **Transient Cyber Assets (TCA) and Removable Media (RM) Protection** section |
| V1.8 | 2022-05-31 | Christine Leung | | | Updated:<br>• Document owner to CIP Program Office (CPO)<br>• Changed "vendor" to "supplier" throughout the document (except specific named documents/forms)<br>• Section 4.1 – IPP and Info Sheet naming to align with published documents<br>• Section 4.3 – Training requirement for BCSI storage location to align with IPP<br>Added:<br>• Section 3 – BCH Responsible Manager<br>Removed:<br>• Section 6.2, bullet b – Duplicate reference or "Medium Impact" with ERC CIP Cyber System(s)<br>• Section 8.3 – Weekly Vendor Revocation Verification pilot has completed and no longer required<br>• Section 10 – Specific procedural language related to physical destruction or degaussing/ magnetic erasure to minimize risk of misalignment with C3 PLCY CORP BES Cyber Asset Reuse and Disposal |

| Version | Revision Date | Author(s) | Reviewer(s) | Approver(s) (Sign-off Date) | Description of Change |
|---|---|---|---|---|---|
| V2.00 | 2023-03-31 | Zaheer Shivji<br>Pak Hui | Anchit Kishore<br>Irina Portnova<br>Denise Pratt<br>Yingzi Zhang<br>Sukriti Aurora<br>Haider Naveed<br>Alya Manansala<br>Ryan Carlson<br>Wafi Kassam<br>Amir Rasti<br>Ben Peco<br>Eva Weclaw | 2023-03-31 | Structural overhaul with technical writer to improve readability.<br>Introduction of CIP-013 related content. |
| V2.01 | 2024-05-21 | Pak Hui | Eva Weclaw<br>Peter Kobzar<br>Mark Christianson | 2024-06-14 | Continuous improvement of CIP-013 requirements. (See Section 9, point B)<br>• Sections 9.1 – 9.3 supports contracts pre-dating this change.<br>• Going forward, Contracts with "NERC CIP Supplementary General Conditions" will guide the suppliers as applicable to the CIP-013 Addendum" |

# 11. Endnotes

[1] CIP-006 R1

[2] CIP-006 R2

[3] CIP-005 R1

[4] CIP-011 R1

[5] CIP-004 R2

[6] CIP-010 R1

[7] CIP-011 R2

[8] CIP-010 R4

[9] CIP-010

[10] CIP-013 All

[11] CIP-013-2 R2

[12] CIP-013 R1.2.1

[13] CIP-013 R1.2.2

[14] CIP-013 R1.2.3

[15] CIP-013 R1.2.3

[16] CIP-005 R2

[17] CIP-013 R1.2.4

[18] CIP-013 R1.2.5

[19] CIP-013 R1.2.6