BC Hydro CIP-013 Addendum for contractors

NERC CIP-013 Cybersecurity Supply Chain Risk Management[1]

Introduction

BC Hydro and Power Authority is committed to regulatory compliance. A component of that commitment is to assess the cybersecurity risk posed by our suppliers when delivering products and/or services to BC Hydro relevant to our critical infrastructure. This is known as "Cybersecurity (Supply Chain) Risk Management".

Obligation

Contractors working for BC Hydro are responsible to meet the expectations specified in their contract, including adherence to BC Hydro rules and standards.

The version of the *Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk*[2] included in this document is designed to provide contractors with an understanding of the cybersecurity supply chain expectations related to their work with BC Hydro. Once a contract is awarded, however, contractors must adhere to our most current procedures.

Prospective contractors must also be familiar with our "NERC CIP Requirements Digest", which is not included in this document.

1 CONTENTS

[1] CIP-013-2 – Cyber Security - Supply Chain Risk Management

[2] "Model Procurement Contract Language Addressing Cybersecurity Supply Chain Risk" (v3 by Edison Electric Institute, "EEI"). See PDF and EEI's sub-page for more information.

2 APPLICABILITY TO BULK ELECTRIC SYSTEM SYSTEM IN BC

Pursuant to directives from BC Utilities Commission ("**BCUC**") and the North American Electric Reliability Corporation ("**NERC**"), BC Hydro is required to set out obligations for suppliers who are in scope of the requirements.

Specific to CIP-013, titled "Cyber Security Cyber Security - Supply Chain Risk Management", BC Hydro has implemented internal policies and procedures for the protection of facilities, systems, assets and information that are critical to the operation or support of the Bulk Electric System ("**BES**"). Collectively these are known as BES Cyber Assets or Systems ("**BCA**" or "**BCS**"). The associated Electronic Access Control or Monitoring Systems ("**EACMS**") and Physical Access Control Systems ("**PACS**") are also included. These designations are identified by BC Hydro in accordance with its internal procedures.

If a Contract relates to BES Cyber Systems (BCS) or BES Cyber System Information ("**BCSI"**), or their associated Electronic Access Control or Monitoring Systems (EACMS) and Physical

Access Control Systems (PACS), and is designated as in scope for CIP-013 requirements, then Contractor must comply with the additional requirements described in this Addendum. This designation will be made clear in the management of new contracts or contract renewals.

3 DEFINITIONS

The following definitions apply only to the terms and conditions in this Addendum.

"**BC Hydro Information**" means for purposes of these terms and conditions, any and all information concerning BC Hydro and its business in any form, including, without limitation, the products and services provided under this Agreement that is disclosed to or otherwise learned by Contractor during the performance of this Agreement.

BES Cyber Asset ("BCA") means Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.

BES Cyber System ("BCS") means one or more BES Cyber Assets logically grouped to perform one or more reliability tasks.

Bulk Electric System ("BES") means, unless modified by NERC documentation and processes, all transmission elements operating at 100 kV or higher and real power and reactive power resources connected at 100 kV or higher. Does not include facilities use in the local distribution of electric energy.

"**Contractor**" or "**Vendor**" or "**Supplier**" means the organization or individual that enters into an agreement with the BC Hydro for supplying a product or service.

"**Contractor Proprietary Information**" means any Contractor information that is considered highly confidential where disclosure outside of the BC Hydro may result in significant loss of Contractor's intellectual property, PII, etc. and may cause damage to the operational effectiveness or otherwise substantially disrupt significant business operations, with examples including but not limited to: source code, private encryption keys, or BC Hydro Information.

"**Disclosed**" means any circumstance when the security, integrity, or confidentiality of any BC Hydro Information has been compromised, including but not limited to incidents where BC Hydro Information has been damaged, lost, corrupted, destroyed, or accessed, acquired, modified, used, or disclosed by any unauthorized person, by any person in an unauthorized manner, or for any unauthorized purpose.

"BCH Responsible Manager" The day-to-day contact and/or work initiator (Hydro's Representative or otherwise as applicable) under the relevant Contract.

"**PII**" means Personally Identifiable Information.

"**Security Incident**" means any circumstance when

(i) Contractor knows or reasonably believes that BC Hydro Information hosted or stored by the Contractor has been Disclosed;

(ii) Contractor knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products and services provided to BC Hydro by Contractor or the physical, technical, administrative, or organizational safeguards protecting Contractor's systems or BC Hydro's systems storing or hosting BC Hydro Information that may affect the BC Hydro Information or that could pose a cyber security risk to the BC Hydro ; or

(iii) Contractor receives any third-party complaint, notice, or communication which relates directly or indirectly to a Security Incident involving

(A) Contractor's handling of BC Hydro Information or Contractor's compliance with the data safeguards in this Agreement or applicable laws; in connection with BC Hydro Information or

(B) a verified impact to the cybersecurity of the products and services provided to BC Hydro that could pose a cybersecurity risk to the BC Hydro

"**Vulnerability**" means a weakness in an information system, system security procedures, internal controls, firmware, software, or implementation that could result in a Security Incident including being exploited or triggered by a threat source.

4 CONFLICT OF TERMS

In case of any conflict between the terms in this CIP-013 Addendum and the terms in the general conditions, the terms of this CIP-013 Addendum will prevail.

5 BC HYDRO REQUIRES SUPPLIERS TO SUPPORT CIP-013 REQUIREMENTS

5.1 NOTIFICATION OF VENDOR IDENTIFIED INCIDENTS

"Notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to BC Hydro (the Responsible Entity)" - CIP-013 R1.2.1.

Contractor Requirements

(A) Contractor agrees to notify BC Hydro as soon as practical, but not later than 24 hour or before 3 pm (PST) of next business day, whichever is sooner, at cybersecurity@bchydro.com by email and the contract's BC Hydro representative (or BCH

Responsible Manager), after Contractor's knowledge of, or reasonable suspicion of, an occurrence of a Security Incident.

(B) The written notice will include the date and time of the Security Incident's occurrence (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a summary of the facts and circumstances of the Security Incident, including a description, to the extent known, of

(a) why the Security Incident occurred (e.g., a description of the reason for the system failure),
(b) the amount and nature of BC Hydro Information known or reasonably believed to have been Disclosed (if applicable), and
(c) the measures being taken to address and remedy the Security Incident and to prevent the same or a similar event from occurring in the future.

(C) Contractor will provide written updates to the initial written notice to BC Hydro addressing any new facts and circumstances learned after the initial written notice is provided and will provide such updates within a reasonable time after learning of those new facts and circumstances.

(D) Contractor will reasonably cooperate with BC Hydro in BC Hydro's efforts to determine the risk posed by the Security Incident to BC Hydro Information and BC Hydro assets.

5.2 Coordination of Responses to Vendor Identified Incidents

"Coordination of responses to vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk to BC Hydro (the Responsible Entity)". – CIP-013 R1.2.2.

Contractor Requirements

5.2.1 Development and Implementation of a Response Plan

Contractor will develop and implement a "Response Plan," which will include policies and procedures to address Security Incidents. The Response Plan will include appropriate provisions for mitigating the harmful effects of Security Incidents and addressing and remedying the occurrence(s) to prevent the recurrence of similar Security Incidents in the future. Contractor will provide BC Hydro access to inspect Contractor's Response Plan, provided that Contractor will have a right to redact any part of the Response Plan that contains Contractor Proprietary Information or information protected by legal privilege.

The development and implementation of the Response Plan will follow industry standard practices, such as those that at a minimum are consistent with the contingency planning requirements of NIST Special Publication 800-61 Rev. 2[3], NIST Special Publication 800-53 Rev.

[3] National Institute of Standards and Technology (NIST), **Computer Security Incident Handling Guide**, Special Publication 800-61 Rev. 2 (2012).

4, CP-1 through CP-13[4] and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended[5].

5.2.2 Prevention of Recurrence

If the Security Incident arises from Contractor-provided software, hardware, or equipment, then, within 60 days of a Security Incident, Contractor will develop and take necessary steps to execute a plan that reduces the likelihood of the same or a similar Security Incident from occurring in the future consistent with the requirements of its Response Plan and industry standards (e.g., NIST Special Publication 800-61 Rev. 2 and NIST Special Publication 800-184, as may be amended[6]) and will communicate to BC Hydro the implementation of such plan to reduce a similar Security Incident.

5.2.3 Coordination of Incident Response with BC Hydro

(a) Contractor will, at its sole cost and expense, assist and cooperate with BC Hydro with respect to any investigation of and response to a Security Incident and disclosures to affected parties in connection with a Security Incident or required under any applicable laws related to a Security Incident.
(b) In the event a Security Incident results in BC Hydro Information being Disclosed such that notification is required to be made to any person or entity, including without limitation any customer, shareholder, or current or former employee of BC Hydro under any applicable laws, including privacy and consumer protection laws, or pursuant to a request or directive from a governmental authority, such notification will be provided by BC Hydro, except as required by applicable law or approved by BC Hydro in writing. BC Hydro will have sole control over the timing and method of providing such notification.

5.3 NOTIFICATION WHEN ACCESS IS NOT NEEDED

"Notification by vendors when remote or onsite access should no longer be granted to vendor representatives". – CIP-013 R1.2.3.

Contractor Requirements

5.3.1 Development and Implementation of Access Control Policy

Contractor will develop and implement policies and procedures to address the security of Contractor's remote and onsite access to BC Hydro Information, BC Hydro systems and

---

[4] NIST, Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication 800- 53 Rev. 4 (2012), note CP-1 through CP-13 cover **Contingency Planning Policy and Procedures, Contingency Plan, Contingency Training, Contingency Plan Testing, Contingency Plan Update, Alternate Storage Site, Alternate Processing Site, Telecommunications Services, Information System Backup, Information System Recovery and Reconstitution, Alternate Communications Protocols, Safe Mode, and Alternative Security Mechanisms.**
[5] NIST Special Publication 800-53 Rev. 4 (2012), note IR-1 through IR-10 cover **Incident Response Policy and Procedures, Incident Response Training, Incident Response Testing, Incident Handling, Incident Monitoring, Incident Reporting, Incident Response Assistance, Incident Response Plan, Information Spillage Response, and Integrated Information Security Analysis Team**
[6] NIST Special Publication 800-61 (Rev. 2) (2012) and NIST, **Guide for Cybersecurity Event Recovery**, Special Publication 800-184 (2016)

networks, and BC Hydro property (an "Access Control Policy") that is consistent with the personnel management requirements of industry standard practices (e.g., NIST Special Publication 800-53 Rev. 4 AC-2[7], PE-2[8], PS-4[9], and PS-5[10] as may be amended) and also meets the following requirements.

5.3.2 BC Hydro Authority Over Access

In the course of furnishing products and services to BC Hydro under this Agreement, Contractor will not access, and will not permit its employees, agents, contractors, and other personnel or entities within its control ("Contractor Personnel") to access BC Hydro's property, systems, or networks or BC Hydro Information without BC Hydro's prior express written authorization. Such written authorization may subsequently be revoked by BC Hydro, at any time in its sole discretion. Further, any Contractor personnel access will be consistent with, and in no case exceed the scope of, any such approval granted by BC Hydro. All BC Hydro-authorized connectivity or attempted connectivity to BC Hydro's systems or networks will be in conformity with BC Hydro's security policies as may be amended from time to time with notice to the Contractor.

5.3.3 Contractor Review of Access

Contractor will review and verify Contractor personnel's continued need for access and level of access to BC Hydro Information and BC Hydro systems, networks and property on a quarterly basis and will retain evidence of the reviews for two year from the date of each review.

5.3.4 Notification and Revocation

Contractor will promptly notify BC Hydro when

(i) any Contractor personnel no longer requires such access in order to furnish the services or products provided by Contractor under this Agreement,
(ii) any Contractor personnel is terminated or suspended or his or her employment is otherwise ended,
(iii) Contractor reasonably believes any Contractor personnel poses a threat to the safe working environment at or to any BC Hydro property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or BC Hydro Information,
(iv) there are any material adverse changes to any Contractor personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record,
(v) any Contractor personnel loses his or her Canadian work authorization, or
(vi) Contractor's provision of products and services to BC Hydro under this Agreement is either completed or terminated, so that BC Hydro can discontinue electronic and/or physical access for such Contractor personnel.

---

[7] NIST Special Publication 800-53 Rev. 4 AC-2 covers **Account Management**
[8] NIST Special Publication 800-53 Rev. 4 PE-2 covers **Physical Access Authorization**
[9] NIST Special Publication 800-53 Rev. 4 PS-4 covers **Personnel Termination**.
[10] NIST Special Publication 800-53 Rev. 4 PS-5 covers **Personnel Transfer**.

Contractor to determine appropriate timing to notify BC Hydro:

- **Urgent**: Email cybersecurity@bchydro.com and the contract's BC Hydro representative (or BCH Responsible Manager) within 24 hour(s) without exceptions for non-business days

- **Routine**: Email SupplyChainNotifications@bchydro.com and the contract's BC Hydro representative (or BCH Responsible Manager) within a timing as agreed to elsewhere in the contract, or consistent with contractor's policy.

Contractor will take all steps reasonably necessary to immediately revoke such Contractor personnel's electronic and physical access to BC Hydro Information as well as BC Hydro property, systems, or networks, including, but not limited to, removing and securing individual credentials and access badges, multifactor security tokens, and laptops, as applicable. Further, for such revoked Contractor personnel, Contractor will return to BC Hydro any BC Hydro-issued property including, but not limited to, BC Hydro photo ID badges, keys, parking passes, documents, or electronic equipment in the possession of such Contractor personnel. Contractor will notify BC Hydro at SupplyChainNotifications@bchydro.com once access to BC Hydro Information as well as BC Hydro property, systems, and networks has been removed.

5.4 Disclosure by Vendors of Known Vulnerabilities

"Disclosure by vendors of known vulnerabilities related to the products or services provided to BC Hydro (the Responsible Entity)" – CIP-013 R1.2.4

Contractor Requirements

5.4.1 Disclosure of Vulnerabilities by Contractor

Contractor will develop and implement policies and procedures to address the disclosure and remediation by Contractor of known Vulnerabilities and defects related to the products and services provided to BC Hydro under this Agreement including the following:

(i) Prior to the delivery of the procured product or service, Contractor will provide summary documentation of publicly disclosed vulnerabilities and material defects in the procured product or services, the potential impact of such vulnerabilities and material defects, the status of Contractor's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Contractor's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

(ii) Supplier will notify BC Hydro by telephone and e-mail of vulnerabilities and material defects in the procured goods or services within fifteen (15) days after such vulnerabilities and material defects become known to Supplier. Supplier will provide summary documentation of vulnerabilities and material defects in the procured goods or services within sixty (60) calendar days after such vulnerabilities and material defects become known to Contractor. This includes

notification of, and summary documentation on, vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the goods or services. The summary documentation will include a description of each vulnerability and material defects and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

(iii) Contractor will disclose the existence of all known methods for bypassing computer authentication in the procured product or services, often referred to as backdoors, and provide written attestation that all such backdoors created by Contractor have been permanently remediated.

(iv) Contractor will implement a vulnerability detection and remediation program consistent with industry standards (e.g., ISO-27417 Vulnerability Disclosure, NIST Cybersecurity Framework v1.1 Reference RS.AN-5[11], NIST Special Publication 800-53 Rev. 4 RA-5[12], SA-11[13], and SI-2[14], as may be amended.)

(v) Contractor will provide the program to BC Hydro for review upon BC Hydro's request.

5.4.2 Disclosure of Vulnerabilities by BC Hydro

Whether or not publicly disclosed by Contractor and notwithstanding any other limitation in this Agreement and following reasonable written notice provided to and acknowledged by Contractor, BC Hydro may disclose any vulnerabilities, material defects, and/or other findings related to the products and services provided by Contractor to:

(a) the Electricity Information Sharing and Analysis Center ("E-ISAC"), the Canadian Centre for Cybersecurity, or any equivalent Canadian governmental entity or program,
(b) to any applicable Canadian governmental entity, upon mutual agreement of BC Hydro and Contractor, when necessary to preserve the reliability of the BES, or
(c) any entity required by applicable law.

5.5 VERIFICATION OF SOFTWARE INTEGRITY AND AUTHENTICITY

"Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System" – CIP-013 R1.2.5

Contractor Requirements

5.5.1 Hardware, Firmware, Software, and Patch Integrity and Authenticity

(a) Contractor will establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided

[11] NIST Cybersecurity Framework v1.1 RS.AN-5 covers **Analysis**
[12] NIST Special Publication 800-53 Rev. 4 RA-5 covers **Vulnerability Scanning**.
[13] NIST Special Publication 800-53 Rev. 4 SA-11 covers **Developer Security Testing and Evaluation**.
[14] NIST Special Publication 800-53 Rev. 4 SI-2 covers **Flaw Remediation.**

under this Agreement, in accordance with industry standards and until otherwise noted with end of sale, end of support, and/or end of life.

(b) Upon request by BC Hydro, Contractor will provide documentation on its: chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on how to request replacement parts, and unless agreed upon elsewhere, commitments to ensure that spare parts will be made available by Contractor.

(c) Upon request by BC Hydro, Contractor will specify how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If BC Hydro deems that it is warranted, Contractor will apply encryption technology to protect procured products throughout the delivery process.

(d) If Contractor provides software or patches to BC Hydro, Contractor will publish or provide a hash conforming to the Federal Information Processing Standard[15] (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2[16]) or similar standard information on the software and patches to enable BC Hydro to use the hash value as a checksum to independently verify the integrity of the software and patches.

(e) Contractor will identify or provide BC Hydro with a method to identify the country (or countries) of origin, of the procured Contractor product and its components (including country of manufacture (hardware) and country of build (software and firmware). Contractor will identify the countries where the development, manufacturing, maintenance, and service for the Contractor product are provided. Contractor will notify BC Hydro of changes in the list of countries where product maintenance or other services are provided in support of the procured Contractor product. This notification in writing will occur at least 180 days prior to initiating a change in the list of countries.

(f) Contractor will provide a software bill of materials for procured (including licensed) products consisting of a list of components and associated metadata that make up a component.

(g) Contractor will use or arrange for the use of trusted channels to ship procured products, such as registered mail and/or tamper-evident packaging for physical deliveries,

(h) Contractor will demonstrate a capability for detecting unauthorized access throughout the delivery process.

(i) Contractor will provide chain-of-custody documentation for procured products appropriate to scope of supply.

5.5.2 Patching Governance

(a) Prior to the delivery of any products and/or services to BC Hydro or any connection of electronic devices, assets, or equipment to BC Hydro's electronic equipment, Contractor will provide documentation regarding the patch management and vulnerability

[15] Federal Information Processing Standards (FIPS), Search | CSRC (nist.gov)
[16] **Security Requirements for Cryptographic Modules**, FIPS 140-2, Security Requirements for Cryptographic Modules | CSRC (nist.gov)

management/mitigation programs and update Contractor's process (including for any third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required by Contractor to be connected to the assets of BC Hydro during the provision of products and services under this Agreement. This documentation will include information regarding:

(i) the resources and technical capabilities to sustain this program and process such as the method or recommendation for how the integrity of a patch is validated by BC Hydro; and

(ii) the approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

(b) Unless otherwise approved by the BC Hydro in writing, products and services supplied by Contractor will not require the use of any out-of-date, unsupported, or end-of-life version of third-party components (e.g., Java, Flash, Web browser, etc.).

(c) Contractor will verify and provide documentation that procured products (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to product or service supply to the o BC Hydro.

(d) In providing the products and services described in this Agreement, Contractor will provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for Contractor products as soon as is practical. Updates to remediate critical vulnerabilities will be provided within a shorter period than other updates, within 7 days. If updates cannot be made available by Contractor within these time periods, Contractor will provide mitigations, methods of exploit detection, and/or workarounds within another 7 days.

(e) In providing third-party hardware, software (including open-source software), and firmware is provided by Contractor to BC Hydro, Contractor will provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses, if such vulnerabilities or weaknesses are applicable to the BC Hydro's use of the third-party product in its system environment, within 30 days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within a shorter period than other updates, within 60 days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested, and made available by Contractor within these time periods, Contractor will provide or arrange for the provision of recommended mitigations and/or workarounds within 30 days.

5.5.3 Viruses Firmware and Malware

(a) Contractor will use reasonable efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to BC Hydro. To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable effort to ensure the third-party investigates whether computer viruses or malware are present in any software or patches providing

them to BC Hydro or installing them on BC Hydro's information networks, computer systems, and information systems.

(b) Contractor warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Contractor will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality. To the extent Contractor is supplying third-party software or patches, Contractor will use reasonable efforts to ensure the third-party will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.

(c) When install files, scripts, firmware, or other Contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor, Contractor must provide or arrange for the provision of technical justification as to why the "false positive" hit has taken place to ensure their code's supply chain has not been compromised.

(d) If a virus or other malware is found to have been coded or otherwise introduced as a direct result of Contractor's breach of its obligations under this Agreement, Contractor will upon written request by BC Hydro and at its own cost:

  (i) Take all commercially reasonable action to eliminate the virus or other malware throughout BC Hydro's information networks, computer systems, and information systems; and

  (ii) If the virus or other malware causes a loss of operational efficiency or any loss of data

    (A) where Contractor is obligated under this Agreement to back up such data, take all commercially reasonable steps necessary and provide all assistance required by BC Hydro and its affiliates, or

    (B) where Contractor is not obligated under this Agreement to back up such data, use commercially reasonable efforts, in each case to mitigate the loss of or damage to such data and to restore the efficiency of such data.

5.5.4 End of Life Operating Systems

(a) Unless otherwise mutually agreed, Contractor-delivered solutions will not be required to reside on end-of-sale, end-of-support, and end-of-life operating systems, or any operating system that is known to be reaching such status six (6) months from the date of installation.

(b) As mutually agreed, Contractor solutions will support the latest versions of operating systems on which Contractor-provided software functions within twenty-four (24) months from official public release of that operating system version.

5.5.5 Cryptographic Requirements

(a) Contractor will document how the cryptographic system supporting the Contractor's products and/or services procured under this Agreement protects the confidentiality,

data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation will include, but not be limited to, the following:
(i) The cryptographic methods[17] and primitives[18] that are implemented in the system, and how these methods are to be implemented.
(ii) The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

(b) Contractor will use only "approved" cryptographic methods as defined in the FIPS 140-2 Standard[19] when enabling encryption on its products.
(c) Contractor will provide or arrange for the provision of an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.
(d) Contractor will ensure that:
(i) As mutually agreed, the system implementation includes the capability for configurable cryptoperiods (the life span of cryptographic key usage) in accordance with the Suggested Cryptoperiods for Key Types found in Table 1 of NIST 800-57 Part 1, as may be amended.
(ii) The key update method supports remote re-keying of all devices within [a negotiated time period(s)] as part of normal system operations.
(iii) Emergency re-keying of all devices can be performed remotely or on-site within 30 days.
(e) Contractor will provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

5.6 Coordination of Controls for Vendor-inititiated Remote Access

"Coordination of controls for (i) vendor-initiated interactive remote access, and (ii) system-to-system remote access with a vendor(s)" – CIP-013 R1.2.6

Contractor Requirements

Contractor will coordinate with BC Hydro on all remote access to BC Hydro's systems and networks, regardless of interactivity, and will comply with any controls for interactive remote access and system-to-system remote access sessions requested by BC Hydro.

5.6.1 Controls for Remote Access

Contractors that directly, or through any of their affiliates, subcontractors, or service providers, connect to BC Hydro's systems or networks agree to the additional following protective measures:

[17] e.g., hash functions, symmetric key algorithms, or asymmetric key algorithms
[18] e.g., Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048
[19] FIPS 140-2 Security Requirements for Cryptographic Modules

(a) Contractor will not access, and will not permit any other person or entity to access, BC Hydro's systems or networks without BC Hydro's written authorization and any such actual or attempted access will be consistent with any such written authorization.
(b) Contractor will implement processes designed to protect credentials as they travel throughout the network and will ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.
(c) Contractor will ensure Contractor Personnel do not use any virtual private network or other device to simultaneously connect machines on any BC Hydro system or network to any machines on any Contractor or third-party systems, without
    (i) using only a remote access method consistent with BC Hydro's remote access control policies,
    (ii) providing BC Hydro with the full name of each individual who uses any such remote access method and the phone number and email address at which the individual may be reached while using the remote access method, and
    (iii) ensuring that any computer used by Contractor personnel to remotely access any BC Hydro system or network will not simultaneously access the Internet or any other third-party system or network while logged on to BC Hydro systems or networks.
(d) Contractor will ensure Contractor Personnel accessing BC Hydro networks are uniquely identified and that accounts are not shared between Contractor personnel.

6 SUPPORTING PROVISIONS

6.1 REQUIREMENTS TO ADDRESS OTHER CYBERSECURITY AND SUPPLY CHAIN RISKS

Contractor Requirements

6.1.1 Contractor Cybersecurity Policy

Contractor will demonstrate to BC Hydro the Contractor's cybersecurity policy which will be consistent with industry standard practices (e.g., NIST Special Publication 800-53 (Rev. 4) as may be amended). Contractor will implement and comply with its established cybersecurity policy.

Any changes to Contractor's cybersecurity policy as applied to products and services provided to BC Hydro under this Agreement and BC Hydro Information will not decrease the protections afforded to BC Hydro or BC Hydro Information and any material changes will be communicated to the BC Hydro in writing by Contractor prior to implementation.

6.1.2 Return or Destruction of BC Hydro Information

Upon the later of (i) completion of the delivery of the products and services to be provided under this Agreement, (ii) the termination of any applicable warranty period under the Agreement or (iii) the termination of this Agreement, Contractor will return to BC Hydro all hardware and removable media provided by BC Hydro containing BC Hydro Information. BC Hydro

Information in such returned hardware and removable media will not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise reasonably directed by BC Hydro. If the hardware or removable media containing BC Hydro Information is owned by Contractor or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity who performed the destruction will be sent to a designated BC Hydro security representative within 15 calendar days after the later of (i) completion of the delivery of the products and services to be provided under this Agreement, (ii) the termination of any applicable warranty period under the Agreement or (iii) the termination of this Agreement. Contractor's destruction or erasure of BC Hydro Information pursuant to this Section will be in compliance with industry standard practices (e.g., Department of Defense 5220-22-M Standard[20], as may be amended).

6.1.3 Audit Rights

Upon request, Contractor will provide to BC Hydro the opportunity to review a copy of the Contractor's policies, procedures, evidence and independent audit report summaries that are part of a cyber security framework (e.g., ISO-27001[21], SOC2[22]). BC Hydro or its third-party designee may, but is not obligated to, perform audits or other tests of Contractor's IT or systems environment and procedural controls to determine Contractor's compliance with the system, network, data, and information security requirements of this Agreement. BC Hydro audits of the Contractor system will be done with at least 30 days advance notice. These audits and tests may include coordinated security tests as mutually agreed to not unduly affect Contractor operations, interviews of relevant personnel, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use, retention, and authorized destruction of BC Hydro Information. Contractor will provide all information reasonably requested by BC Hydro in connection with any such audits and will provide reasonable access and assistance to BC Hydro upon request. Contractor will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. BC Hydro reserves the right to view, upon request, any original security reports that Contractor has undertaken or commissioned to assess Contractor's own network security. Any regulators of BC Hydro or its affiliates will have the same rights of audit as described herein upon request.

6.1.4 Regulatory Examinations

Contractor agrees that any regulator or other governmental entity with jurisdiction over BC Hydro and its affiliates may examine Contractor's activities relating to the performance of its obligations under this Agreement to the extent such authority is granted to such entities under the applicable law. Contractor will promptly cooperate with and provide all information reasonably requested by the regulator or other governmental entity in connection with any such examination and provide reasonable assistance and access to equipment, records, networks, and systems reasonably requested by the regulator or other governmental entity. Contractor

[20] DoD 5220.22-M **Data Erasure Standard** – a widely recognized and implemented data destruction method.
[21] ISO 27001 - **Information Security Management**
[22] **Service Organization Control** (SOC) audit on how a cloud-based service provider handles sensitive information

agrees to comply with reasonable recommendations that result from such regulatory examinations within reasonable timeframes at Supplier's sole cost and expense.

7 REVISION LOG

Version	Date	Description of Change
1	June 2024	First release

End of document