APPENDIX A

CYBERSECURITY REQUIREMENTS

This Appendix A forms part of the Contract, and in the event of a conflict with the Contract, this Appendix A will govern.

1. **Definitions**. The following definitions apply only to the terms and conditions in this Appendix.

a. "***CEII***" means Critical Energy Infrastructure Information and/or Critical Electric Infrastructure Information

b. "***Company Information***" means for purposes of these terms and conditions, any and all information concerning Company and its business in any form, including, without limitation, the Goods and Services provided under the Contract that is disclosed to or otherwise learned by Seller during the performance of the Contract.

c. "***Disclosed***" means any circumstance when the security, integrity, or confidentiality of any Information has been compromised, including but not limited to incidents where Company 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.

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

e. "***Security Incident***" means any circumstance when (i) Seller knows or reasonably believes that Company Information hosted or stored by the Seller has been Disclosed; (ii) Seller knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the Goods and Services provided to Company by Seller or the physical, technical, administrative, or organizational safeguards protecting Seller's systems or Company's systems storing or hosting Company Information; or (iii) Seller receives any complaint, notice, or communication which relates directly or indirectly to a Security Incident involving (A) Seller's handling of Company Information or Seller's compliance with the data safeguards in the Contract or applicable laws; in connection with Company Information or (B) the cybersecurity of the Goods and Services provided to Company by Seller.

f. "***Seller's Proprietary Information***" means any Seller information that is considered highly confidential where disclosure outside of the Company may result in significant loss of Seller'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 Company Information.

2. **Notification of Vendor-Identified Security Incidents**. Seller agrees to notify Company's Access Administration Group by calling (902) 428-6683 and by email with a read receipt to itsec.ops@nspower.ca whenever it becomes aware of the occurrence of a Security Incident, but in no case later than twenty-four (24) hours of such awareness; a written notice shall also be sent by email to Seller's primary business contact with Buyer. The notice shall 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 detailed summary of the facts and circumstances of the Security Incident, including a description of (a) why the Security Incident occurred (e.g., a description of the reason for the

system failure), (b) the amount of Company Information known or reasonable believed to have been Disclosed, and (c) the measure being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

Seller shall provide written updates of the notice to Company addressing any new facts and circumstances learned after the initial written notice is provided and shall provide such updates within a reasonable time after learning of those new facts and circumstances.

Seller shall reasonably cooperate with Company in Company's efforts to determine the risk posed by the Security Incident, including providing additional information regarding the Security Incident upon request from the Buyer.

3. **<u>Coordinate of Responses to Cybersecurity Incidents</u>**.

a. <u>Response Plan</u>. Seller shall develop and implement a "Response Plan," which shall include policies and procedures to address Security Incidents. The Response Plan shall 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. Seller shall provide Company access to inspect Seller's Response Plan. The development and implementation of the Response Plan shall 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, NIST Special Publication 800-53 Rev. 4, CP-1 through CP-13 and the incident response requirements of NIST Special Publication 800-53 Rev. 4, IR-1 through IR-10 as those standards may be amended.

Immediately upon learning of a Security Incident related to the Goods and Services provided to Buyer, Seller shall implement its Response Plan and, within 24 hours of implementing its Response Plan, shall notify Company in writing of that implementation as described above.

b. <u>Prevention of Recurrence</u>. Within five (5) days of a Security Incident, Seller shall develop and 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,) and shall communicate that plan to Buyer. Seller shall provide recommendations to Company on actions that Company may take to assist in the prevention of recurrence, as applicable or appropriate.

c. <u>Coordination of Incident Response with Buyer</u>. Within five (5) days of notifying Company in writing of the Security Incident, Seller shall recommend actions to be taken by Company on Company-controlled systems to reduce the risk of a recurrence of the same or a similar Security Incident, including, as appropriate, the provision of action plans and mitigating controls. Seller shall coordinate with Company in developing those action plans and mitigating controls. Seller will provide Company guidance, recommendations, and other necessary information for recovery efforts and long-term remediation and/or mitigation of cyber security risks posed to Company Information, equipment, systems, and networks as well as any information necessary to assist Company in relation to the Security Incident.

d. Notification to Affected Parties.

i. Seller will, at its sole cost and expense, assist and cooperate with Company with respect to any investigation of a Security Incident, disclosures to affected parties, and other remedial measures as requested by Company in connection with a Security Incident or required under any applicable laws related to a Security Incident.

ii. In the event a Security Incident results in Company 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 Company 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 Buyer, except as required by applicable law or approved by Company in writing. Company will have sole control over the timing and method of providing such notification.

e. Unrelated Security Events. In the event:

i. Seller Proprietary Information, related to the Goods and Services provided to the Company under the Contract, has been corrupted or destroyed without authorization or has been accessed, acquired, compromised, modified, used, or disclosed by any unauthorized person, or by any person in an unauthorized manner or for an unauthorized purpose;

ii. Seller knows or reasonably believes that an act or omission has compromised the cybersecurity of the Goods and Services provided by Seller to an entity other than Buyer; or

iii. Seller receives any valid complaint, notice, or communication which relates directly or indirectly to (a) Contract's handling of Seller Proprietary Information or Sellers' compliance with applicable law in accordance with Seller Proprietary information or (b) the cybersecurity of the Goods and Services provided by Seller to an entity other than Company (collectively an "Unrelated Security Incident"),

Seller shall provide to Company a confidential report describing, to the extent legally permissible, a detailed summary of the facts and circumstances of the Unrelated Security Incident, including a description of (1) why the Unrelated Security Incident occurred, (2) the nature of the Seller's Proprietary Information disclosed, and (3) the measures being taken to address and remedy the occurrence to prevent the same or a similar event from occurring in the future.

4. Access Control

a. Development and Implementation of Access Control Policy. Seller shall develop and implement policies and procedures to address the security of Seller's remote and onsite access to Company Information, Company systems and networks, and Company 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, PE-2, PS-4, and PS-5 as may be amended) and also meets the following requirements:

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

c. Seller Review of Access. Seller will review and verify Seller personnel's continued need for access and level of access to Company Information and Company systems, networks and property on a quarterly basis and will retain evidence of the reviews for two years from the date of each review.

d. Notification and Revocation. Seller will immediately notify Company in writing, via email to itsec.ops@nspower.ca is acceptable, but under no circumstances later than close of business on the same day as the day of termination or change set forth below, when:

i. any Seller personnel no longer requires such access in order to furnish the Goods and Services provided by Seller under the Contract,

ii. any Seller personnel is terminated or suspended or his or her employment is otherwise ended,

iii. Seller reasonably believes any Seller personnel poses a threat to the safe working environment at or to any Company property, including to employees, customers, buildings, assets, systems, networks, trade secrets, confidential data, and/or Company Information,

iv. there are any material adverse changes to any Seller personnel's background history, including, without limitation, any information not previously known or reported in his or her background report or record,

v. any Seller personnel loses his or her Canadian work authorization, or

vi. Seller's provision of Goods and Services to Company under the Contract is either completed or terminated, so that Company can discontinue electronic and/or physical access for such Seller personnel.

Seller will take all steps reasonably necessary to immediately revoke such Seller personnel electronic and physical access to Company Information as well as Company 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 Seller personnel, Seller will return to Company any Company-issued property including, but not limited to, Company photo ID badges, keys, parking passes, documents, or electronic equipment in the possession of such Seller personnel. Seller will notify Company at itsec.ops@nspower.ca and by phone at (902) 428-6683 once access to Company Information as well as Company property, systems, and networks has been removed.

5. Disclosure and Remediation of Vulnerabilities

a. Disclosure and Remediation by Contractor. Seller shall develop and implement policies and procedures to address the disclosure and remediation by Seller of vulnerabilities and material defects related to the Goods and Services provided to Company under the Contract including the following:

i. Prior to the delivery of the procured Goods and Services, Seller shall provide or direct Company to an available source of summary documentation of publicly disclosed vulnerabilities and material defects in the procured Goods and Services, the potential impact of such vulnerabilities and material defects, the status of Seller's efforts to mitigate those publicly disclosed vulnerabilities and material defects, and Seller's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds.

ii. Seller shall provide or direct Company to an available source of summary documentation of vulnerabilities and material defects in the procured Goods and Services within thirty (30) calendar days after such vulnerabilities and material defects become known to Seller. The summary documentation shall include a description of each vulnerability and material defect and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds (e.g., monitoring).

iii. Seller shall disclose the existence of all known methods for bypassing computer authentication in the procured Goods and Services, often referred to as backdoors, and provide written attestation that all such backdoors created by Seller have been permanently remediated.

b. Disclosure of Vulnerabilities by Buyer. Whether or not publicly disclosed by Seller and notwithstanding any other limitation in the Contract, Company may disclose any Vulnerabilities, material defects, and/or other findings related to the Goods and Services provided by Seller to (a) the Electricity Information Sharing and Analysis Center ("E-ISAC"), the United States Cyber Emergency Response Team ("CERT"), or any equivalent U.S. governmental entity or program, (b) to any applicable U.S. governmental entity when necessary to preserve the reliability of the BES as determined by Company in its sole discretion, or (c) any entity required by applicable law.

6. Software and Patch Integrity and Authenticity

a. Hardware, Firmware, Software and Patch Integrity and Authenticity.

i. Seller shall establish, document, and implement risk management practices for supply chain delivery of hardware, software (including patches), and firmware provided under the Contract. Seller shall 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 commitments to ensure that for one (1) year spare parts shall be made available by Seller.

ii. Seller shall specify how digital delivery for procured Goods and Services (*e.g.*, software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. If Company deems that it is warranted, Seller shall apply encryption technology to protect procured Goods and Services throughout the delivery process.

iii. If Seller provides software or patches to Buyer, Seller shall publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable Company to use the hash value as a checksum to independently verify the integrity of the software and patches.

iv. Seller shall identify or provide Company with a method to identify the country (or countries) of origin of the procured Seller Goods and Services and its components (including hardware, software, and firmware). Seller will identify the countries where the development, manufacturing, maintenance, and service for the Seller Goods and Services are provided. Seller will notify Company of changes in the list of countries where Goods and Services maintenance or other services are provided in support of the procured Seller Goods and Services. This notification in writing shall occur at least 180 days prior to initiating a change in the list of countries.

v. Seller shall provide a software bill of materials for procured (including licensed) Goods and Services consisting of a list of components and associated metadata that make up a component.

vi. Seller shall use or arrange for the use of trusted channels to ship procured Goods and Services, such as Canadian registered mail and/or tamper-evident packaging for physical deliveries.

vii. Seller shall demonstrate a capability for detecting unauthorized access throughout the delivery process.

viii. Seller shall demonstrate chain-of-custody documentation for procured Goods and Services as determined by Company in its sole discretion and require tamper-evident packaging for the delivery of this hardware.

b. <u>Patching Governance</u>.

i. Prior to the delivery of any products and/or services to Company or any connection of electronic devices, assets, or equipment to Company's electronic equipment, Seller shall provide documentation regarding the patch management and vulnerability management/mitigation programs and update process (including third-party hardware, software, and firmware) for products, services, and any electronic device, asset, or equipment required by Seller to be connected to the assets of Company during the provision of Goods and Services under the Contract. This documentation shall include information regarding:

a) 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 Buyer; and

b) the approach and capability to remediate newly reported zero-day vulnerabilities for Seller Goods and Services.

ii. Unless otherwise approved by the Company in writing, the current or supported version of Seller Goods and Services supplied by Seller shall not require the use of out-of-date, unsupported, or end-of-life version of third-party components (*e.g.*, Java, Flash, Web browser, etc.).

iii. Seller shall verify and provide documentation that procured Goods and Services (including third-party hardware, software, firmware, and services) have appropriate updates and patches installed prior to delivery to Buyer.

iv. In providing the Goods and Services described in the Contract, Seller shall provide or arrange for the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for Seller Goods and Services within 30 days. Updates to remediate critical vulnerabilities shall be provided within a shorter period than other updates, within seven (7) days. If updates cannot be made available by Seller within these time periods, Seller shall provide mitigations, methods of exploit detection, and/or workarounds within seven (7) days.

v. When third-party hardware, software (including open-source software), and firmware is provided by Seller to Buyer, Seller shall provide or arrange for the provision of appropriate hardware, software, and/or firmware updates to remediate newly discovered vulnerabilities or weaknesses, if applicable to the Company'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 Seller's use of the third-party product in its system environment shall be provided within a shorter period than other updates, within thirty (30) days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested, and made available by Seller within these time periods, Seller shall provide or arrange for the provision of recommended mitigations and/or workarounds within 30 days.

c. Virus, Firmware and Malware.

i. Seller 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 Buyer. To the extent Seller is supplying third-party software or patches, Seller 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 Company or installing them on Company's information networks, computer systems, and information systems.

ii. Seller warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Seller 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 Seller is supplying third-party software or patches, Seller 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.

iii. When install files, scripts, firmware, or other Seller-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, Seller 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.

iv. If a virus or other malware is found to have been coded or otherwise introduced as a direct result of Seller's breach of its obligations under the Contract, Seller shall upon written request by Company and at its own cost:

a) Take all necessary remedial action and provide assistance to Company to eliminate the virus or other malware throughout Company's information networks, computer systems, and information systems; and

b) the virus or other malware causes a loss of operational efficiency or any loss of data (A) where Seller is obligated under the Contract to back up such data, take all steps necessary and provide all assistance required by Company and its affiliates, or (B) where Seller is not obligated under the Contract 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.

d. <u>End of Life Operating Systems</u>

i. Seller-delivered solutions will not be required to reside on end-of-life operating systems, or any operating system that will go end-of-life six (6) months from the date of installation.

ii. Seller solutions will support the latest versions of operating systems on which Seller-provided software functions within twenty-four (24) months from official public release of that operating system version.

e. <u>Cryptographic Requirements</u>

i. Seller shall document how the cryptographic system supporting the Seller’s Goods and Services procured under the Contract protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system. This documentation shall include, but not be limited to, the following:

a) The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (*e.g.*, Secure Hash Algorithm [SHA]- 256, Advanced Encryption Standard [AES]-128, RSA, and Digital Signature Algorithm [DSA]-2048) that are implemented in the system, and how these methods are to be implemented.

b) The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.

ii. Seller will use only “approved” cryptographic methods as defined in the FIPS 140-2 Standard when enabling encryption on its products.

iii. Seller shall provide or arrange for the provision of an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

iv. Seller shall ensure that:

a) 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.

b) The key update method supports remote re-keying of all devices within one (1) year as part of normal system operations.

c) Emergency re-keying of all devices can be remotely performed within 30 days.

v. Seller shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

7. Remote Access Controls

Seller shall coordinate with Company on all remote access to Company's systems and networks, regardless of interactivity, and shall comply with any controls for interactive remote access and system-to-system remote access sessions requested by Buyer.

a. Controls for Remote Access. Contractors that directly, or through any of their affiliates, subcontractors, or service providers, connect to Company's systems or networks agree to the additional following protective measures:

i. Seller will not access, and will not permit any other person or entity to access, Company's systems or networks without Company's written authorization and any such actual or attempted access will be consistent with any such written authorization.

ii. Seller shall implement processes designed to protect credentials as they travel throughout the network and shall ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials.

iii. Seller shall ensure Seller Personnel do not use any virtual private network or other device to simultaneously connect machines on any Company system or network to any machines on any Seller or third-party systems, without

a) using only a remote access method consistent with Company's remote access control policies,

b) providing Company 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

c) ensuring that any computer used by Seller personnel to remotely access any Company system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Company systems or networks.

iv. Seller shall ensure Seller Personnel accessing Company networks are uniquely identified and that accounts are not shared between Seller personnel.

8. Seller Cybersecurity Policy.

Seller will provide to Company the Seller’s cybersecurity policy which shall be consistent with industry standard practices (e.g., NIST Special Publication 800-53 (Rev. 4) as may be amended). Seller will implement and comply with its established cybersecurity policy.

Any changes to Seller’s cybersecurity policy as applied to Goods and Services provided to Company under the Contract and Company Information shall not decrease the protections afforded to Company or Company Information and any material changes shall be communicated to the Company in writing by Seller prior to implementation.

9. Return or Destruction of Company Information.

Upon completion of the delivery of the Goods and Services to be provided under the Contract, or at any time upon Company's request, Seller will return to Company all hardware and removable media provided by Company containing Company Information. Company Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise directed by Buyer. If the hardware or removable media containing Company Information is owned by Seller or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction will be sent to a designated Company security representative within thirty (30) calendar days after completion of the delivery of the Goods and Services to be provided under the Contract, or at any time upon Company's request. Seller's destruction or erasure of Company Information pursuant to this Section shall be in compliance with industry standard practices (*e.g.*, Department of Defense 5220-22-M Standard, as may be amended).

10. **Audit Rights**.

Upon request, Seller shall provide to Company the opportunity to review a copy of the Seller's policies, procedures, evidence and independent audit report summaries that are part of a cyber security framework (e.g. ISO-27001, SOC2). Company or its third-party designee may, but is not obligated to, perform audits and security tests of Seller's IT or systems environment and procedural controls to determine Contractor's compliance with the system, network, data, and information security requirements of the Contract. Company audits of the Seller system shall be initiated with at least 30 days advance notice. These audits and tests may include coordinated security tests as mutually agreed to not unduly affect Seller 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 Company Information. Seller shall provide all information reasonably requested by Company in connection with any such audits and shall provide reasonable access and assistance to Company upon request. Seller will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. Company reserves the right to view, upon request, any original security reports that Seller has undertaken or commissioned to assess Contractor's own network security. If requested, copies of these reports will be sent via bonded courier to Company security contact. Seller will notify Company of any such security reports or similar assessments once they have been completed. Any regulators of Company or its affiliates shall have the same rights of audit as described herein upon request.

11. **Regulatory Examinations**.

Seller agrees that any regulator or other governmental entity with jurisdiction over Company and its affiliates may examine Contractor's activities relating to the performance of its obligations under the Contract to the extent such authority is granted to such entities under the law. Seller shall 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 all equipment, records, networks, and systems reasonably requested by the regulator or other governmental entity. Seller agrees to comply with all reasonable recommendations that result from such regulatory examinations within reasonable timeframes.

12. Risk Assessment Questionnaire.

Seller shall be required to complete and submit to Company a Risk Assessment Questionnaire ("Questionnaire") upon request. Upon submission, Seller represents and warrants that the responses provided to the Questionnaire are complete and accurate. Seller shall notify Company immediately upon becoming aware that any responses to the Questionnaire are false or no longer hold true, and upon Company's request, Seller shall complete a new or updated Questionnaire, in whole or in part as indicated by Buyer. To the extent information requested by the Questionnaire is made publicly available by Seller, Seller may direct Company so such information; upon Company's review and determination of adequacy, such information may be deemed acceptable by Company in lieu of completing the Questionnaire.

13. Reseller Services.

To the extent Seller provides reseller services and is not the original provider ("OEM") of the services, software, equipment or other Goods and Services procured under the Contract, Seller shall:

a. Provide reasonable assistance as necessary to facilitate discussions between Company and the OEM;
b. Shall assist Company in securing completion of any Questionnaires or other risk-related documents as required by Buyer;
c. Shall ensure that the OEM complies with the terms and conditions of this Appendix A including but not limited to securing the OEM's signature on this Appendix A to verify compliance;
d. Provide any additional and reasonable assistance with respect to ensuring and verifying OEM compliance with this Appendix A as may be reasonably requested by Company from time to time.