CYBER SECURITY APPENDIX

Available in accessible formats upon request

V1 2018 09 21

1 INTERPRETATION

1.1 In this Appendix the following words and phrases shall have the following meanings. Words and phrases that are capitalized in this Appendix and not defined below have the meaning given elsewhere in the Contract. Headings are used for convenience only, and do not affect the interpretation or application of matters under consideration.

"Appendix" means this Appendix and all schedules attached hereto.

"Person" shall be broadly interpreted to include, without limitation, any corporation, partnership, other entity, or individual.

"Cyber Asset(s)" means: (i) a Programmable Electronic Device owned by, or under the control of, the Purchaser; and/or as the case may be, (ii) a Programmable Electronic Device to be provided (and/or which is provided) by the Contractor to the Purchaser under the Contract.

"Cyber Asset Information" means information, regardless of form, format or medium, concerning any Cyber Asset(s). Examples of Cyber Asset Information include, without limitation, operational procedures, inventories, network topology or similar diagrams, facility floor plans, equipment layouts, disaster recovery plans, incident response plans, and security configuration information.

"Programmable Electronic Device(s)" includes: (i) an electronically programmable or configurable device; and (ii) a communication network. Examples of Programmable Electronic Devices include, without limitation, computer hardware, computer software, media and data, communication means and pathways, and related systems and networks.

2 GENERAL

2.1 In addition to, and without invalidating or otherwise affecting any other term or condition of the Contract, the Contactor shall perform, execute, and deliver the Work and the Contract, in accordance with this Appendix.

2.2 The Contractor is responsible for, and shall ensure compliance with, the terms, conditions, and requirements of this Appendix, by the Contractor and all Persons engaged in the Work under the Contractor including, without limitation, the Contractor, subcontractors, and all employees and agents of any of the same. The Contractor shall bind all subcontractors to written agreements containing obligations no less stringent than those assumed by the Contractor under this Appendix.

3 CONFIDENTIALITY

3.1 In addition to, and without invalidating or otherwise affecting any other term or condition of the Contract, the Contractor shall:

(a) keep Cyber Asset Information confidential;

(b) not, without the prior written consent of the Purchaser, disclose or otherwise make available any Cyber Assets, or any Cyber Asset Information, to any Person other than in accordance with this Appendix;

(c) not use Cyber Asset Information for any purpose other than in connection with the performance of the Contractor's obligations under the Contract; and

(d) not use Cyber Assets for any purpose other than in connection with the performance of the Contractor's obligations under the Contract.

3.2 The Contractor shall restrict access to Cyber Assets and Cyber Asset Information to only those of its employees who have a need to know/access any of the same to carry out obligations under the Contract; provided that, before such access, such employees have been informed of the confidential nature of the Cyber Assets and Cyber Asset Information in question.

3.3 The Contractor may provide access to Cyber Assets and Cyber Asset Information to subcontractors of the Contractor who have a need to know/access the same to carry out obligations under the Contract; provided that, before access is provided, such Person(s) has agreed in writing to be bound by obligations no less stringent than those assumed by the Contractor under this Appendix.

3.4 The Contractor shall be liable for the failure of any Person, for which access to/disclosure of Cyber Assets and Cyber Asset Information is given pursuant to Section 3.2 and Section 3.3 above, to comply with the requirements of Article 3.

3.5 The Contractor acknowledges that any failure to comply with the provisions of this Article 3, shall cause irreparable harm to the Purchaser which cannot be adequately compensated for in damages, and accordingly acknowledges that the Purchaser shall be entitled, in addition to any other remedies available to it, interlocutory and permanent injunction relief to restrain any anticipated, present, or continuing breach of this Article 3.

4 SECURITY PRACTISE REQUIREMENTS

4.1 Without limiting or otherwise affecting the generality or application of any other term or condition of the Contract and this Appendix, the Contractor shall:

(a) secure Cyber Assets and Cyber Asset Information against unauthorized or accidental access, damage, disclosure, or attack;

(b) deliver to the Purchaser written notice immediately upon the discovery of an event described in Section 4.1(a) above.

(c) comply with the written directions of the Purchaser in respect of the investigation, remedying, and prevention, of any matter/event described in Section 4.1(a) above.

(d) secure and control Cyber Assets and Cyber Asset Information while in transit;

(e) secure Cyber Assets and Cyber Asset Information by at least one (1) method of physical security, ensuring continuous monitoring. Non-exclusive examples of methods of physical security are facility access controls such as card access door, room or cabinet lock, security guard and sign-in system, or alarmed intrusion detection system;

(f) secure Cyber Assets and Cyber Asset Information by at least one (1) mechanism of cyber security, ensuring continuous monitoring and logging functions. Non-exclusive examples of mechanisms of cyber security are a firewall, access control such as password protection, strong encryption, access monitoring and logging, or alarmed intrusion detection system;

(g) authenticate all physical and cyber access to Cyber Assets and Cyber Asset Information;

(h) secure connections to/from equipment used to transfer Cyber Asset Information by means of physical and cyber security. Non-exclusive examples of means of such physical and cyber security are use of dedicated communications lines, password protection, strong encryption, no split tunnel, no wireless communications of Cyber Asset Information, and access management systems;

(i) maintain the integrity of Cyber Asset Information;

(j) transfer Cyber Asset Information only on secured systems and only when required for Contractor’s performance of obligations under the Contract;

5 RESTRICTED ACCESS FOR INDIVIDUALS

5.1 Access to Cyber Assets and Cyber Asset Information shall be restricted on a strictly need-to-know basis. Individuals performing obligations under the Contract must only be granted access to such Cyber Assets and Cyber Asset Information that are required for their performance of such obligations under the Contract.

5.2 The Contractor shall revoke access for an individual to Cyber Assets and Cyber Asset Information and notify the Purchaser:

(a) if an individual is terminated for cause, within 24 hours of such termination; and

(b) if an individual no longer requires access for performing obligations under the Contract, within seven (7) days from the time access is no longer required.

6 PERSONNEL RISK ASSESSMENT

6.1 All individuals who are or may be engaged in the performance of the Contract shall, at the discretion and direction of the Purchaser, be required to undergo and successfully pass, to Purchaser's satisfaction, a personnel risk assessment. The Purchaser may conduct or may require the Contractor to conduct, from time to time, personnel risk assessment(s) on such individuals and the Contractor shall cause each such individual to authorize and comply with the requirements of the Purchaser in respect of same.

6.2 The Purchaser has the right to require the Contractor to permanently remove any individual engaged in the performance of the Work for reasons including, but not limited to, failure of such individual to pass a personnel risk assessment to the Purchaser's satisfaction, unsatisfactory performance, or failure to comply with the Purchaser's corporate policies or procedures. The Contractor shall, at no cost to the Purchaser, engage a satisfactory replacement for any such individual.

6.3 The Contractor shall ensure that:

(a) all individuals who have or will have access to Cyber Assets or Cyber Asset Information have been previously cleared by a personnel risk assessment, to the Purchaser's satisfaction, before being allowed such access;

(b) any change to the criminal record status of any such individual(s) is reported to the Purchaser immediately; and

(c) when Purchaser performed PRA completion is mandated, completed forms are submitted by each such individual to the Purchaser.

7 TRAINING

7.1 All individuals who are or may be engaged in the performance of the Contract shall, depending on regulatory requirements of the Purchaser from time to time, be required to undergo training concerning, generally, the use, access, and handling of Cyber Assets and Cyber Asset Information, all to the Purchaser's satisfaction. The Purchaser may conduct or may require the Contractor to conduct, from time to time, such training, and the Contractor shall cause such individual(s) to authorize and comply with the requirements of the Purchaser in respect of same. The form, content, and requirements for any training shall be established, from time to time, by the Purchaser. The Purchaser shall provide the Contractor with notice(s) of such requirements.

8 RECORDS

8.1 The Contractor shall create and maintain complete and accurate books and records in respect of its obligations under this Appendix, including books and records concerning:

(a) all individuals who have and/or require physical or cyber access to any Cyber Assets and Cyber Asset Information, including, a description of the type, rights, and point, of access for each individual and cross-referenced to the individual's responsibilities in performance of obligations under the Contract;

(b) personnel risk assessments scheduled and completed pursuant to Section 6.1 above (with results) for all individuals having and/or requiring access to Cyber Assets or Cyber Asset Information;

(c) processes and procedures used to control, administer, and log, activities, practices, procedures, and communications, of the Contractor in respect of its obligations under this Appendix;

(d) such other matters that the Purchaser may direct the Contractor, from time to time, in writing.

8.2 The Contractor shall update records made pursuant to Section 8.1 (a) above within seven (7) days of any change of any individual's access type(s) or right(s), and providing a description of the reason for access change and the date of same.

9 INSPECTION

9.1 The Contractor shall, on reasonable prior notice from the Purchaser, grant the Purchaser, and its authorized representative's, access to the Contractor's facilities, lands, and premises, and those of its subcontractors and suppliers, at any time during normal business hours, to enable such representatives to verify that the Contractor and any other Person(s) are in compliance with the requirements of this Appendix.

9.2 On reasonable prior notice, the Purchaser may attend any facilities, lands or premises and inspect and audit books and records required herein and may take copies of any such books and records. Further, when directed by the Purchaser, the Contractor shall deliver to the Purchaser copies of any such books and records.

10 DELIVERY OF PROPERTY

10.1 Upon completion of the Work or such other time(s) as directed by the Purchaser, the Contractor shall deliver to the Purchaser any property owned by, or under the control of, the Purchaser.

11 DELIVERY OR DESTRUCTION OF CYBER ASSET INFORMATION

11.1 At the direction and option of the Purchaser, the Contractor shall either destroy or deliver promptly to the Purchaser all copies of Cyber Asset Information which are in the possession or control of the Contractor; and certify in writing to the Purchaser that such destruction or delivery has been completed.

12 APPLICATION

12.1 The expiry or termination the Contract shall not affect or prejudice any rights or obligations that have accrued or arisen under this Appendix prior to expiry or termination, and those rights and obligations shall survive the expiry or termination of the Contract. Subject to Section 13 below, the provisions of this Appendix and all other provisions of the Contract necessary to give effect thereto shall survive the expiry or termination of the Contract.

13 WAIVER

13.1 The Purchaser may, from time to time in the Purchaser's sole discretion, waive in writing any term, condition, or requirements of this Appendix, or the Contractor's continued obligation(s) in respect thereof. No such waiver shall be effective unless it is in writing and signed by the Purchaser.