REQUEST FOR PROPOSALS: SCHEDULE 1
DEMANDE DE PROPOSITION: ANNEXE 1

Note: This Schedule is appended to Part 6 and Part 7 of the Request for Proposals
Remarque: Cette Annexe est ajoutée à la Partie 6 and Partie 7 de la Demande de propositions.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

1.1 Security Requirements

a. Prior to award of contract, the following conditions must be met:

For Foreign Suppliers:

i. The Bidders must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html .

ii. The Bidders must provide proof that they are incorporated or authorized to do business in their jurisdiction as indicated in Part 7 - Resulting Contract Clauses.

iii. The Bidders will need to provide assurance that it can receive and store **CANADA PROTECTED** information/assets on its site or premises as indicated in Part 7 – Resulting Contract Clauses, Annex A and the listed IT Security Requirements.

iv. (a) The Bidder's proposed location of work performance and document safeguarding must meet the security requirement as indicated in Part 7 – Resulting Contract Clauses.

(b) The Bidders must provide the addresses of the proposed site(s) or premise(s) of work performance and/or document safeguarding.

v. Bidders are reminded to obtain the required security clearance promptly as the Work must not be started without the requisite security clearances. Any delay in the award of a contract to allow the successful bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

vi. In the case of a joint venture Bidder, each member of the joint venture must meet the security requirements.

vii. Bidders are reminded that Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED** information related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

viii. The Bidders must ensure that all the databases used by organizations to provide the services described in the SOW containing any **CANADA PROTECTED** information, related to the Work, are located within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a in a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-eng.html .

ix. The bid must clearly indicate the work which the Bidder plans to subcontract. All subcontracting arrangements which provide the subcontractor with access to any Canadian restricted sites and/or access to **CANADA PROTECTED** information/assets are subject to approval by Canada. The description of subcontracting arrangements must demonstrate how the Bidder will ensure that all requirements, terms, conditions, and clauses of the contract are met.

PART 7 - RESULTING CONTRACT CLAUSES

7.5 Security Requirements

The following security requirements apply to and form part of the contract.

A. SECURITY REQUIREMENTS FOR CANADIAN SUPPLIERS: Provided by CISD/PWGSC

B. SECURITY REQUIREMENTS FOR FOREIGN SUPPLIERS:

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Works and Government Services Canada (PWGSC), administered by International Industrial Security Directorate (IISD), PWGSC. The Canadian DSA is the authority for confirming Foreign recipient **Contractor / Subcontractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the Foreign recipient **Contractor / Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering outside of Canada the services listed and described in the subsequent **Contract / Subcontract**.

1. The Foreign recipient **Contractor / Subcontractor** must be from a Country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html.

2. The Foreign recipient **Contractor / Subcontractor** must provide proof that they are incorporated or authorized to do business in their jurisdiction.

3. The Foreign recipient **Contractor / Subcontractor** must provide assurance that it can receive and store **CANADA PROTECTED** information/assets on its site or premises as indicated in Annex A and as listed in the Information Technology Security Requirements.

4. (a) The Foreign recipient **Contractor's / Subcontractor's** proposed location of work performance must meet the security requirement as indicated in Annex A and as listed in the IT Security Requirements.

   (b) The Foreign recipient **Contractor / Subcontractor** must provide the address(es) of the proposed site(s) or premise(s) of work performance and/or document safeguarding.

5. The Foreign recipient **Contractor / Subcontractor** defined as an individual or legal entity possessing the legal capacity to enter into a contract, shall provide confirmation of compliance with the below terms and conditions, in writing, to the Canadian Designated Security Authority (DSA), prior to the execution of the works, services or performance, of which requires or involves **access to Canadian restricted sites and/or access to CANADA PROTECTED information/assets.**

6. The Foreign **Contractor / Subcontractor** shall not begin the work, services or performance until the Canadian Designated Security Authority (DSA) is satisfied that all contract security requirement conditions have been met. Canadian DSA confirmation shall be provided, in writing, to the Foreign recipient **Contractor / Subcontractor** in an Attestation Form, to provide confirmation of compliance and authorization for services to be performed.

7. All **CANADA PROTECTED** information/assets provided or generated under this **Contract / Subcontract** will continue to be safeguarded in the event of withdrawal by the recipient party or upon termination of the **Contract / Subcontract**, in accordance with the national policies of the supplier's country.

8. The Foreign recipient **Contractor / Subcontractor** shall provide the **CANADA PROTECTED** information/ assets a degree of safeguarding no less stringent than that provided by the Government of Canada in accordance with the National Policies, National Security legislation and regulations and as prescribed by the Canadian DSA.

9. All **CANADA PROTECTED** information/assets provided to the Foreign recipient **Contractor / Subcontractor** pursuant to this **Contract / Subcontract** by the Government of Canada, shall be marked by the Foreign recipient **Contractor / Subcontractor** with the equivalent security classification utilized by the supplier's country and in accordance with the national policies of the supplier's country.

10. The Foreign recipient **Contractor / Subcontractor** shall, at all times during the performance of this **Contract / Subcontract**, ensure the transfer of **CANADA PROTECTED** information /assets be facilitated through the Canadian DSA.

11. Upon completion of the Work, the Foreign recipient **Contractor / Subcontractor** shall return to the Government of Canada, all **CANADA PROTECTED** information/assets furnished or produced pursuant to this **Contract / Subcontract**, including all **CANADA PROTECTED** information/assets released to and / or produced by its subcontractors.

12. The Foreign recipient **Contractor / Subcontractor** must identify an authorized Contract Security Officer (CSO) to be responsible for the overseeing of the security requirements, as defined in this contract. This individual will be appointed by the proponent Foreign recipient Contractor's Chief Executive officer or Designated Key Senior Official, defined as an owner, officer, director, executive, and or partner who occupy a position which would enable them to adversely affect the organization's policies or practices in the performance of the contract.

13. The Foreign recipient **Contractor/ Subcontractor** shall not permit **access to Canadian restricted sites or grant access to CANADA PROTECTED A information**, except to its personnel subject to the following conditions:

    a) Personnel have a need-to-know for the performance of the **Contract / Subcontract**;

    b) Personnel have been subject to a criminal record check, with favourable results, from a recognized Governmental agency in **their country** as well as a background verification. The approved verifications for the required criminal record check and background verification are listed at Appendix A;

    c) The Foreign **Contractor / Subcontractor** will ensure that its Chief Executive Officer (CEO) or Senior Official of the company will appoint a Contract Security Officer (CSO) and/or an Alternate Contract Security Officer (ACSO) in order to ensure compliance with all contracting security requirements;

    d) The Foreign recipient **Contractor / Subcontractor** shall ensure that personnel provide consent to share results of the Criminal record Background Check with the Canadian DSA and other Canadian Government Officials, if requested;

    e) The Government of Canada reserves the right to deny access to **CANADA PROTECTED** information/assets to a Foreign **Contractor / Subcontractor** for cause.

14. **CANADA PROTECTED** information/assets provided or generated pursuant to this **Contract / Subcontract** shall not be further provided to a third party Foreign recipient Subcontractor unless:

a. written assurance is obtained from the Canadian DSA to the effect that the third-party Foreign recipient Subcontractor has been approved for access to **CANADA PROTECTED** information/assets by the Canadian DSA; and

b. written consent is obtained from the Canadian DSA, if the third-party Foreign recipient Subcontractor is located in a third country.

15. The Foreign recipient **Contractor / Subcontractor** must ensure that all the databases used by organizations to provide the services described in the SOW containing any **CANADA PROTECTED** information, related to the Work, are located within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a in a country with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PWGSC website: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-eng.html .

16. The Foreign recipient **Contractor / Subcontractor** MUST NOT utilize its Information Technology systems to electronically process, produce, or store on a computer system and transfer via an IT link any **CANADA PROTECTED** information/assets until the Canadian DSA has granted approval to do so. After approval has been granted in writing to the Foreign recipient **Contractor / Subcontractor**, these tasks may be performed up to the level of **CANADA PROTECTED A**.

    See **Annex ___ for IT Security Requirements**.

17. The Foreign recipient **Contractor / Subcontractor** shall not use the **CANADA PROTECTED** information/assets for any purpose other than for the performance of the **Contract / Subcontract** without the prior written approval of the Government of Canada. This approval must be obtained from the Canadian Designated Security Authority (DSA).

18. The Foreign recipient **Contractor / Subcontractor** requiring access to Canadian Government site(s), under this contract, will submit a Request for Site Access to the Departmental Security Officer of the Canadian Radio-television and Telecommunications Commission.

19. The Foreign recipient **Contractor / Subcontractor** shall immediately report to the Canadian Designated Security Authority (DSA) all cases in which it is known or there is reason to suspect that **CANADA PROTECTED information** / assets pursuant to this **Contract / Subcontract** has been compromised.

20. The Foreign recipient **Contractor / Subcontractor** shall immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that **CANADA PROTECTED** information/assets accessed by the Foreign recipient **Contractor / Subcontractor**, pursuant this **Contract / Subcontract**, have been lost or disclosed to unauthorized persons.

21. The Foreign recipient **Contractor / Subcontractor** shall not disclose the **CANADA PROTECTED** information to a third party government, person, firm or representative thereof, without the prior

written consent of the Government of Canada. Such consent shall be sought through the Canadian DSA.

22. In the event that a Foreign recipient **Contractor / Subcontractor** is chosen as a supplier for this Contract, subsequent Country-Specific Foreign security requirement clauses shall be generated and promulgated by the Canadian DSA, and provided to the Government of Canada Contracting Authority, to ensure compliance with the security provisions, as defined by the Canadian DSA, in relation to equivalencies.

23. The Foreign recipient **Contractor / Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex _____.

24. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of the Canadian DSA.

25. Canada has the right to reject any request to electronically access, process, produce, transmit or store **CANADA PROTECTED** information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

Annex A

The Foreign recipient **Contractor / Subcontractor** shall also insert this Annex A into all contracts/subcontracts into which it enters that involve access to **CANADA PROTECTED** information / assets.

Physical Security Conditions:

The paragraphs below describe the minimum requirements for the treatment of **CANADA PROTECTED** information/assets. Further specifications respecting the conditions listed below for physical security may be provided subsequent to a compliance visit if required to identify shortcomings and define the required safeguarding measures to ensure comparability with Canadian standards for the processing, production and storage of **CANADA PROTECTED** information/assets. It is the responsibility of the Foreign recipient **Contractor / Subcontractor** to identify potential threats to the environment and ensure compliance with identified security requirements.

Document Safeguarding - Physical Security:

The Foreign recipient **Contractor / Subcontractor** shall transfer all **CANADA PROTECTED** information processed, produced or stored pursuant to this **contract / subcontract** in a single sealed envelope with no security marking only through registered mail of a national postal service or as specified in writing by the Canadian DSA.

The Foreign recipient **Contractor / Subcontractor** shall mark all **CANADA PROTECTED** information/assets generated pursuant to this **contract / subcontract** as **"CANADA PROTECTED"** in the upper right corner of the face of the document, and in accordance with the Security Requirement Check list as provided.

In accordance with Article 504 of Chapter 5 of the Canadian Government "Contract Security Manual", the Foreign recipient **Contractor / Subcontractor** is responsible for ensuring compliance with the following physical safeguarding measures:

1. Storage:

a. As a minimum, **CANADA PROTECTED** information/assets shall be stored in a locked container in an Operations Zone; and

b. **CANADA PROTECTED** information/assets shall not be stored in the same container as negotiable or attractive assets.

2. Keys for containers:

a. Keys (devices such as instruments, cards, combinations and code numbers used to open and close containers) shall be safeguarded, commensurate with the highest level of sensitivity of the information to which they provide access. This also applies to recorded information that would allow a key to be produced;

b. When a key is issued, the recipient must sign for the key. The number of the key, the location of the container it opens, and the name of the recipient shall be recorded and kept by the Foreign recipient **Contractor's / Subcontractor's** Contract Security Officer (CSO);

c. The Foreign recipient **Contractor's / Subcontractor's** CSO shall maintain a record of the dates of, and reasons for all key or lock changes; and

d. Assigned keys should be changed:

   i. at least every twelve (12) months;
   ii. when those with access to the container no longer require access; and
   iii. when a container has been or may have been compromised, the locking mechanism must be changed immediately.

3. Precautions during use:

Special care must be taken to safeguard against unauthorized access when **CANADA PROTECTED** information/assets are removed from approved storage containers. Specific points to observe are as follows:

a. do not leave **CANADA PROTECTED** information/assets unattended;
b. ensure that **CANADA PROTECTED** information/assets cannot be viewed; and
c. ensure that discussion of **CANADA PROTECTED** information/assets cannot be overheard by persons not holding the appropriate level of clearance, and /or do not have a need-to-know.

Information Technology Systems:

In accordance with security measures required for the treatment and access to **CANADA PROTECTED** information, the following describes the minimum security requirements for processing, producing and storing **CANADA PROTECTED** information on information systems:

a. **Access:** Physical access to all hardware elements of the IT system is to be strictly controlled.

b. **Identification and Authentication (ID&A):** All information systems shall have the following functionality:

   i. Up-to-date list of authorized users.
   ii. Positive identification of all users at the start of each processing session.

c. **Passwords:** Passwords to access the information system are required. Passwords shall be a minimum of 6 characters long (9 is preferable) and shall include numeric and "special" characters (if permitted by the information system) as well as alphabetic characters.

d. **Internal Access Control**: All information systems shall have internal access controls to prevent unauthorized users from accessing or modifying the data.

e. **Data Transmission**: **CANADA PROTECTED** information must be transmitted or accessed electronically (e.g. point to point computer links) via a public network like the internet, only with the use of approved commercial encryption devices validated by the Canadian DSA.

f. **Security Accounting and Audit:** Security relevant events fall into two categories, namely "legitimate events" and "violations".

   i. The following types of events shall always be recorded:

      a. All log on attempts whether successful or failed;
      b. All log off (including time out where applicable);
      c. The creation, deletion or alteration of access rights and privileges; and
      d. The creation, deletion or alteration of passwords.

   ii. For each of the events listed above, the following information is to be recorded:

      a. Type of event;
      b. User ID;
      c. Date and Time; and
      d. Device ID.

The accounting records shall be stored in a facility to provide the information System Manager with a hard copy of all or selected activity. There shall also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need-to-know.

If the operating system is unable to provide this, then the equipment shall be protected by physical means when not in use (i.e. locked away or the hard drive removed and locked away).

g. **Integrity and Availability:** The following supporting measures shall be implemented:

i. Provide general protection against normally foreseeable accidents, mishaps and known recurrent problems (e.g. viruses and power supply variations);
ii. Defined Business Contingency Plan;
iii. Data backup with local storage; and
iv. Anti Virus Software (implementation, with updates, of an acceptable industry standard Anti-virus software).

h. **Logon Banners**: Wherever possible, a "Logon Banner" shall be provided to summarize the requirements for the information system, which may be utilized to institute legal action in case of any breach occurring. A suggested format for the text is below:
"Unauthorized access to this computer system may constitute a criminal offense".

i. **Unattended Terminals:** Authorized users are to be automatically logged off the system if their terminals have been inactive for a predetermined period of time, or their terminals must activate a password protected screen saver after 15 minutes of inactivity, to prevent an attacker making use of an unattended terminal.

j. **Internet Connections:** Computer systems shall not be connected directly to the Internet unless protected by a firewall (a software personal firewall is the minimum).

k. **Disposal:** Before IT storage media (e.g. disks) are disposed of, an erasure product shall be used to overwrite the data. This is a more thorough process than deletion of files.

APPENDIX A

The Foreign recipient **Contractor / Subcontractor** must perform a security screening of all its personnel who will need access to **Canadian restricted sites and/or access to CANADA PROTECTED A information/assets**:

a) Identity check:
   i. Copies of two of valid original pieces of government issued identity documentation, one of which must include a photo
   ii. Surname (last name)

iii. Full given names (first name) – underline or circle usual name used
iv. Family name at birth
v. All other names used (aliases)
vi. Name changes
    1. Must include the name they changed from and the name they changed to, the place of change and the institution changed through
vii. Sex
viii. Date of birth
ix. Place of birth (city, province/state/region, and country)
x. Citizenship(s)
xi. Marital status/common-law partnership
    1. Current status (married, common-law, separated, widowed, divorced, single)
    2. All current spouses (if applicable)
        a. Surname (last name)
        b. Full given names (first name) – underline or circle usual name used
        c. Date and duration of marriage/common-law partnership
        d. Date of birth
        e. Family name at birth
        f. Place of birth (city, province/state/region, and country)
        g. Citizenship(s)

b) Residency check:
    i. The last five (5) years of residency history starting from most recent with no gaps in time.
        1. Apartment number, street number, street name, city, province or state, postal code or zip code, country, from-to dates.

c) Educational check:
    i. The educational establishments attended and the corresponding dates.

d) Employment history check:
    i. The last five (5) years of employment history starting from most recent with no gaps in time.
    ii. Three (3) employment reference check from the last five (5) years.

e) Criminal records check:
    i. Report(s) containing all criminal convictions for the last five (5) years in and outside of the candidate's country of residence.

f) Credit check:
    i. Credit check report where available.

PARTIE 6 - EXIGENCES DE SÉCURITÉ, EXIGENCES FINANCIÈRES ET AUTRES EXIGENCES

1.1 Exigences de sécurité:

(a) Avant l'attribution d'un contrat, les conditions suivantes doivent être respectées:

Pour les fournisseurs canadiens : Fourni par CISD/TPSGC

Pour les fournisseurs étrangers:

i. Les soumissionnaires doivent être dans un pays de l'Union européenne, dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational. Le programme de sécurité des contrats (PSC) à des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de TPSGC: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

ii. Les soumissionnaires devront fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence dans leur juridiction, comme indiqué dans la partie 7 - Clauses du contrat subséquent.

iii. Les soumissionnaires devront fournir l'assurance qu'ils peuvent recevoir et entreposer sur place des renseignements/biens **CANADA PROTÉGÉS**, comme il est indique à la partie 7 – Clause du contrat subséquent, Annexe A et dans les exigences de sécurité informatique.

iv. (a) Le lieu proposé pour les travaux et pour la protection des documents doit satisfaire aux exigences relatives à la sécurité comme indiqué dans la partie 7 - Clauses du contrat subséquent;

(b) Les soumissionnaires doivent fournir les adresses des sites proposés ou des locaux de travail et la sauvegarde des documents.

v. On rappelle au soumissionnaire d'obtenir rapidement la cote de sécurité requise, puisque les travaux ne doivent pas commencer tant qu'il n'aura pas obtenu les attestations de sécurité appropriées. La décision de retarder l'attribution du contrat, pour permettre au soumissionnaire retenu d'obtenir les attestations de sécurité appropriées, demeure à l'entière discrétion de l'autorité contractante.

vi. Dans le cas d'un soumissionnaire en coentreprise, chaque membre de l'entreprise commune doit satisfaire aux exigences de sécurité.

vii. Les soumissionnaires sont rappelés que le Canada a le droit de rejeter toute demande visant l'accès électronique, le traitement, la production ou l'entreposage de renseignements **CANADA PROTÉGÉS**

liés aux travaux dans un autre pays s'il y a des raisons de croire que leur sécurité, leur confidentialité ou leur intégrité pourrait être menacée.

viii. Les soumissionnaires doivent s'assurer que toutes les bases de données utilisées par les organisations pour offrir les services décrits à l'énonce de travaux contenant des renseignements **CANADA PROTÉGÉS** liés aux travaux se trouvent dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinationaldans ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational. Le programme de sécurité des contrats (PSC) a des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de TPSGC: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-fra.html.

ix. La proposition doit clairement indiquer les travaux pour lesquels l'entrepreneur prévoit soumissionner. Tous les contrats de sous-traitance dans lesquels il est prévu que le sous-traitant aura accès à des renseignements/biens **CANADA PROTÉGÉS** sont assujettis à l'approbation du Canada. La description des contrats de sous-traitance doit indiquer comment le soumissionnaire assurera le respect des exigences, des modalités, des conditions et des clauses du contrat.

PARTIE 7 - CLAUSES DU CONTRAT SUBSÉQUENT

7.5 Exigences relatives à la Sécurité

Les exigences de sécurité suivantes s'appliquent et font partie du contrat.

A. EXIGENCES RELATIVES À LA SÉCURITÉ POUR ENTREPRENEUR CANADIEN: Fourni par CISD/TPSGC

B. EXIGENCES RELATIVES À LA SÉCURITÉ POUR ENTREPRENEUR ÉTRANGER :

L'Autorité désignée en matière de sécurité pour le Canada (ADS canadien) pour les questions industrielles au Canada est la Direction de la sécurité industrielle internationale (DSII), Secteur de la sécurité industrielle (SSI), Travaux publics et Services gouvernementaux Canada (TPSGC). L'ADS canadien est chargée d'évaluer la conformité **des entrepreneurs / des sous-traitants** étrangers destinataires aux exigences en matière de sécurité pour les fournisseurs étrangers. Les exigences en matière de sécurité suivantes s'appliquent **à l'entrepreneur / aux sous-traitants** étranger destinataires, incorporés ou autorisés à faire des affaires dans un état autre que le Canada et qui assurent la prestation de services décrites dans **le contrat / le contrat de sous-traitance** ultérieur.

1. **L'entrepreneur/Le sous-traitant** étranger destinataire doivent être dans un pays de l'Union européenne, dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatérale ou multinationale. Le programme de sécurité industrielle a des ententes en matière de sécurité industrielle, protocole d'entente bilatérale ou multinationale industrielle avec les pays mentionnés au site de TPSGC suivant: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-fra.html.

2. **L'entrepreneur / Le sous-traitant** étranger destinataire doit fournir une preuve qu'il est incorporé ou autorisé à faire affaire dans son champ de compétence.

3. **L'entrepreneur / Le sous-traitant** étranger destinataire doit fournir l'assurance qu'il peut recevoir et entreposer sur place des renseignements/biens **CANADA PROTÉGÉS**, comme il est indiqué à l'Annexe A et tel qu'indiqué dans les exigences de sécurité informatique.

4. (a) Le lieu proposé pour les travaux et pour la protection des documents doit satisfaire aux exigences relatives à la sécurité comme il est indiqué à l'Annexe A et tel qu'indiqué dans les exigences de sécurité informatique.

   (b) **L'entrepreneur / Le sous-traitant** étranger destinataire doit fournir l'adresse du ou des lieux proposés pour la réalisation des travaux et/ou pour la protection des documents.

5. **L'entrepreneur / Le sous-traitant** étranger destinataire, c'est-à-dire le particulier ou la personne morale qui a la capacité juridique de passer un marché, doit fournir une preuve écrite de conformité avec les modalités ci-dessous à l'administration désignée en matière de sécurité (ADS) canadienne avant l'exécution des travaux, la prestation des services ou toute autre prestation qui exige ou prévoit **l'accès à des lieux à accès restreint situés au Canada et/ou accès a des renseignements/biens CANADA PROTÉGÉS.**

6. **L'entrepreneur / Le sous-traitant** étranger destinataire ne doit pas entreprendre les travaux, fournir les services ou assurer toute autre prestation tant que l'Administration désignée en matière de sécurité au Canada (ADS canadienne) n'a pas confirmé le respect de toutes les conditions et exigences en matière de sécurité stipulées dans le contrat. L'ADS canadienne donne cette confirmation par écrit **à l'entrepreneur / au sous-traitant** étranger destinataire. Un Formulaire d'attestation remis par l'ADS canadienne **à l'entrepreneur / au sous-traitant** étranger destinataire permettra de confirmer la conformité et l'autorisation de fournir les services prévus.

7. Dans l'éventualité du retrait de la partie destinataire ou à la fin **du contrat/ du contrat de sous-traitance**, tous les renseignements et les biens de niveau **CANADA PROTÉGÉS** fournis ou produits en vertu **du présent contrat/ du présent contrat de sous-traitance** continueront d'être protégés, conformément aux politiques nationales du pays des fournisseurs.

8. **L'entrepreneur / Le sous-traitant** étranger destinataire assurera une protection des renseignements et des biens de niveau **CANADA PROTÉGÉS** aussi stricte que celle mise en œuvre par le gouvernement du Canada, conformément aux politiques, aux lois et aux règlements nationaux en matière de sécurité nationale, et comme prévu par l'ADS de Canada.

9. **L'entrepreneur/ Le sous-traitant** étranger destinataire doit attribuer à tous les renseignements et biens de niveau **CANADA PROTÉGÉ**S qui lui sont fournis par le gouvernement du Canada en vertu **du présent contrat/ du présent contrat de sous-traitance** la cote de sécurité équivalente utilisée par les pays des fournisseurs, conformément aux politiques nationales du pays des fournisseurs.

10. **L'entrepreneur / Le sous-traitant** étranger destinataire doit, en tout temps durant l'exécution **du contrat / du contrat de sous-traitance**, veiller à ce que le transfert des renseignements et des biens de niveau **CANADA PROTÉGÉS** soit facilité par l'ADS de Canada.

11. À la fin des travaux, **L'entrepreneur / Le sous-traitant** étranger destinataire doit restituer au gouvernement du Canada tous les renseignements et les biens de niveau **CANADA PROTÉGÉ** qu'il aura reçus ou produits en vertu **du présent contrat / du présent contrat de sous-traitance**, y compris tous les renseignements et les biens de niveau **CANADA PROTÉGÉS** remis à ses sous-traitants ou produits par eux.

12. **L'entrepreneur / Le sous-traitant** étranger destinataire proposé doit identifier l'agent de sécurité du contrat (ASC) autorisé qui sera responsable du contrôle des exigences de sécurité, telles qu'elles sont définies dans le présent contrat. Cette personne sera désignée par le président-directeur général ou par un cadre supérieur clé de l'entreprise étrangère destinataire proposée. Les cadres supérieurs clés comprennent les propriétaires, les agents, les directeurs, les cadres et les partenaires occupant un poste qui leur permettrait d'avoir une influence sur les politiques ou les pratiques de l'organisation durant l'exécution du contrat.

13. **L'entrepreneur / Le sous-traitant** étranger destinataire n'autorisera pas l'accès **à des lieux à accès restreint au Canada ni à des renseignements de niveau CANADA PROTÉGÉS A**, sauf à son personnel, sous réserve des conditions suivantes:

    a. Le personnel a un besoin de savoir pour l'exécution **du contrat / du contrat de sous-traitance**.

    b. Le personnel a fait l'objet d'une vérification du casier judiciaire et une vérification d'antécédents, avec des résultants favorables, d'une agence gouvernementale reconnue **dans leur pays**. Les vérifications approuvées pour le casier judiciaire et des antécédents requis sont énumérés à l'Appendice A;

c. **L'entrepreneur / Le sous-traitant** étranger destinataire doit faire le nécessaire pour que le président-directeur général (PDG) ou le cadre supérieur clé désigné (CSCD) de l'entreprise nomme un agent de sécurité d'entreprise (ASE) et un agent remplaçant de sécurité d'entreprise (ARSE) qui veilleront au respect de toutes les exigences en matière de sécurité stipulées dans le contrat;

d. **L'entrepreneur / Le sous-traitant** étranger destinataire doit s'assurer que le personnel consente à la divulgation du casier judiciaire et antécédents à l'ADS canadienne et d'autres fonctionnaires du gouvernement canadien, si demandé;

e. Le Gouvernement du Canada se réserve le droit de refuser l'accès aux renseignements et / ou des biens niveau **CANADA PROTEGÉS** à **l'entrepreneur / au sous traitant** étranger pour cause.

14. Les renseignements et les biens de niveau **CANADA PROTÉGÉS** fournis ou produits dans le cadre **du présent contrat / du présent contrat de sous-traitance** ne doivent pas être remis à un autre sous-traitant étranger destinataire, sauf dans les cas suivants:

a) L'ADS canadienne atteste par écrit que le sous-traitant étranger destinataire a obtenu l'accès aux renseignements et biens de niveau **CANADA PROTÉGÉS** par l'intermédiaire de l'ADS canadienne;

b) L'ADS Canadienne donne son autorisation écrite lorsque l'autre sous-traitant destinataire étranger est situé dans un autre pays.

15. Les soumissionnaires doivent s'assurer que toutes les bases de données utilisées par les organisations pour offrir les services décrits à l'énonce de travaux contenant des renseignements **CANADA PROTÉGÉS** liés aux travaux se trouvent dans un pays de l'organisation du traité de l'Atlantique Nord (OTAN) ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinationaldans ou dans un des pays avec lesquels le Canada a conclu une entente en matière de sécurité industrielle et un protocole d'entente bilatéral ou multinational. Le programme de sécurité des contrats (PSC) a des ententes en matière de sécurité industrielle, protocole d'entente bilatéral ou multinational industrielle avec les pays mentionnés au site suivant de TPSGC: http://ssi-iss.tpsgc-pwgsc.gc.ca/gvrnmnt/risi-iisr-fra.html.

16. **L'entrepreneur / Le sous-traitant** étranger destinataire NE DOIT PAS utiliser ses systèmes de technologie de l'information pour traiter, produire ou stocker dans un système informatique et transferer au moyen d'un lien électronique des renseignements de niveau **CANADA PROTÉGÉS** avant que l'ADS du Canada lui en donne le droit. Une fois que **l'entrepreneur / le sous-traitant** étranger destinataire a reçu cette approbation écrite, il peut effectuer ces tâches jusqu'au niveau **CANADA PROTÉGÉ A**.

Voir l'**Annexe ____ pour les exigences de sécurité informatique**.

17. **L'entrepreneur/ Le sous-traitant** étranger destinataire ne doit pas utiliser les renseignements ni les biens de niveau **CANADA PROTÉGÉS** pour répondre à des besoins distincts de l'exécution **du contrat/ du contrat de sous-traitance** sans l'approbation écrite préalable du gouvernement du Canada. Cette autorisation doit être obtenue auprès de l'administration désignée en matière de sécurité (ADS) du Canada.

18. **L'entrepreneur/Le sous-traitant** étranger destinataire recevant l'accès aux sites du gouvernement canadiens, en vertu du présent contrat, soumettra une demande d'accès au site à l'agent de sécurité ministériel du Conseil de la radiodiffusion et des télécommunications canadiennes.

19. **L'entrepreneur / Le sous-traitant** étranger destinataire doit signaler immédiatement à l'administration désignée en matière de sécurité (ADS) canadienne tous les cas pour lesquels il sait ou il a lieu de croire que des biens et/ou des renseignements de niveau **CANADA PROTÉGÉS** obtenus dans le cadre **du présent contrat / du présent contrat de sous-traitance** ont été compromis.

20. **L'entrepreneur / Le sous-traitant** étranger destinataire doit immédiatement signaler à l'ADS canadienne tous les cas dans lesquels il sait ou il a lieu de croire que des renseignements ou des biens de niveau **CANADA PROTÉGÉS** fournis ou produits **par l'entrepreneur / le sous-traitant** étranger destinataire conformément **au présent contrat / au présent contrat de sous-traitance** ont été perdus ou divulgués à des personnes non autorisées.

21. **L'entrepreneur/ Le sous-traitant** étranger destinataire ne doit pas divulguer les renseignements de niveau **CANADA PROTÉGÉS** à un tiers, qu'il s'agisse d'un gouvernement, d'un particulier, d'une entreprise ou de ses représentants, sans l'accord écrit préalable du gouvernement du Canada. Cet accord doit être obtenu par l'ADS du Canada.

22. Si un **entrepreneur / sous-traitant** étranger destinataire est choisi comme fournisseur dans le cadre de ce contrat, des clauses de sécurité propres a son pays seront établies et mises on œuvre par l'ADS canadienne; ces clauses seront fournies à l'autorité contractante du gouvernement du Canada, afin de respecter les dispositions de sécurité relatives aux équivalences établies par l'ADS canadienne.

23. **L'entrepreneur / Le sous-traitant** étranger destinataire doit se conformer aux dispositions de la Liste de vérification des exigences relatives à la sécurité figurant à l'Annexe _____.

24. Les contrats de sous-traitance comportant des exigences relatives à la sécurité NE doivent PAS être attribués sans l'autorisation écrite préalable de l'ADS canadienne.

25. Le Canada a le droit de rejeter toute demande visant l'accès électronique, le traitement, la production ou l'entreposage de renseignements/biens **CANADA PROTÉGÉS** liés aux travaux dans un autre pays s'il y a des raisons de croire que leur sécurité, leur confidentialité ou leur intégrité pourrait être menacée.

ANNEXE A

L'entrepreneur / Le sous-traitant étranger destinataire doit intégrer la présente Annexe A à tous les **contrats / contrats de sous-traitance** qu'il conclut et qui prévoient l'accès des renseignements/biens de niveau **CANADA PROTÉGÉS**.

Conditions de sécurité matérielle :

Les paragraphes ci-dessous décrivent les exigences minimales pour le traitement des informations et des actifs **CANADA PROTÉGÉS**. D'autres spécifications concernant les conditions énumérées ci-dessous pour la sécurité physique peuvent être fournies suite à une visite de conformité si nécessaire pour identifier les défauts et définir les mesures de sauvegarde nécessaires pour assurer la comparabilité avec les normes canadiennes pour le traitement, la production et l'entreposage des informations et des actifs **CANADA PROTÉGÉS**. Il incombe **à l'entrepreneur / au sous-traitant** étranger destinataire d'identifier les menaces potentielles pour l'environnement et d'assurer la conformité aux exigences de sécurité identifiées.

Protection des documents – Sécurité matérielle :

L'entrepreneur / Le sous-traitant étranger destinataire doit transférer tous les renseignements de niveau **CANADA PROTÉGÉS** traités, produits ou archivés dans le cadre **du présent contrat / du présent contrat de sous-traitance** dans une enveloppe simple scellée, sans mention de la cote de sécurité, uniquement au moyen du courrier recommandé d'un service postal national ou selon les exigences précisées par écrit par l'ADS canadienne.

L'entrepreneur / Le sous-traitant étranger destinataire doit apposer sur tous les renseignements de niveau **CANADA PROTÉGÉS** produits dans le cadre **du présent contrat / du présent contrat de sous-traitance** la mention **« CANADA PROTÉGÉS »** dans le coin supérieur droit du recto du document et conformément à la Liste de vérification des exigences relatives à la sécurité qui lui a été remise.

Aux termes de l'article 504 du Manuel de la sécurité contractuelle du gouvernement du Canada, **l'entrepreneur / le sous-traitant** étranger destinataire doit veiller à la conformité des mesures de sécurité matérielle suivantes :

1. Archivage :

a. Les renseignements/biens de niveau **CANADA PROTÉGÉS** doivent être conservés, à tout le moins, dans un contenant fermant à clé situé dans une zone de travail.

b. Les renseignements/biens de niveau **CANADA PROTÉGÉS** ne doivent pas être conservés dans le même contenant que des effets négociables ou des biens attrayants.

2. Clés des armoires :

a. Les clés (et les dispositifs comme les instruments, les cartes, les combinaisons et les numéros de code utilisés pour ouvrir ou fermer les armoires) doivent être protégées selon le niveau de confidentialité le plus élevé des renseignements ou des biens auxquels elles donnent accès. Cette disposition s'applique également aux renseignements enregistrés qui permettraient de produire une clé.

b. Lorsqu'on remet une clé, on doit demander à la personne qui la reçoit d'apposer sa signature dans un registre. On doit noter dans ce registre, que l'agent de sécurité d'entreprise **de l'entrepreneur / du sous-traitant** étranger destinataire doit conserver, le numéro de la clé, les coordonnées de l'armoire qu'elle permet d'ouvrir et le nom du destinataire de cette clé.

c. L'agent de sécurité d'entreprise **de l'entrepreneur / du sous-traitant** étranger destinataire doit tenir un registre des dates et des motifs de chaque changement de clé ou de serrure.

d. Les clés remises devraient être changées :

   i. au moins une fois tous les 12 mois;
   ii. quand les personnes qui ont accès à l'armoire n'ont plus besoin d'y avoir accès;
   iii. lorsqu'on a tenté ou pu essayer d'ouvrir une armoire, le mécanisme de verrouillage doit être changé immédiatement.

3. Précautions à prendre pendant l'utilisation des renseignements:

Il faut prendre des mesures particulières pour protéger les renseignements/biens de niveau **CANADA PROTÉGÉS** contre l'accès non autorisé lorsqu'on les sort des armoires ou des conteneurs autorisés. Il faut surveiller en particulier les points suivants:

a. On ne doit pas laisser sans surveillance des renseignements/biens de niveau **CANADA PROTÉGÉS**.
b. Il faut empêcher la consultation de renseignements/biens de niveau **CANADA PROTÉGÉS**.
c. Il faut prendre les mesures nécessaires pour que des personnes qui n'ont pas l'attestation de sécurité appropriée ou qui n'ont aucun « besoin de savoir » ne puissent pas entendre des discussions sur des renseignements/biens de niveau **CANADA PROTÉGÉS**.

Systèmes de technologie de l'information :

Conformément aux mesures de sécurité exigées pour traiter les renseignements de niveau **CANADA PROTÉGÉS A et/ou B** et y avoir accès, les exigences minimales de sécurité prévues pour traiter, produire

et archiver des renseignements de niveau **CANADA PROTÉGÉS A et/ou B** à l'aide de systèmes d'information sont décrites dans la présente section.

a. **Accès :** L'accès physique à toutes les composantes matérielles du système de TI doit être strictement contrôlé.

b. **Identification et authentification :** Tous les systèmes d'information doivent comprendre les fonctions suivantes:

   i. Une liste à jour des utilisateurs autorisés.
   ii. Un mécanisme d'identification positive de tous les utilisateurs au début de chaque session de traitement.

c. **Mots de passe** : Des mots de passe sont obligatoires pour avoir accès au système d'information. Les mots de passe doivent être formés d'au moins six caractères (une chaîne de neuf caractères est préférable) et comprendre des lettres, des chiffres et des caractères « spéciaux » (si le système d'information le permet).

d. **Contrôle d'accès interne** : Tous les systèmes d'information doivent être dotés de contrôles d'accès internes afin d'empêcher des utilisateurs non autorisés d'avoir accès aux données ou de les modifier.

e. **Transmission des données** : Les renseignements de niveau **CANADA PROTÉGÉS** doivent être transmis ou consultés de façon électronique (par des liaisons informatiques point-à-point) par l'intermédiaire d'un réseau public, comme Internet, au moyen exclusivement de dispositifs de chiffrement commerciaux approuvés et validés par l'ADS canadienne.

f. **Comptes rendus et vérifications de la sécurité** : Les événements relatifs à la sécurité peuvent être classés en deux catégories : les événements légitimes et les infractions.

   i. Les types d'événements suivants doivent toujours être consignés:

      a. Toutes les tentatives d'ouverture de session, qu'elles soient fructueuses ou non.
      b. Toutes les fins de session (y compris après un délai d'inactivité).
      c. La création, la suppression ou la modification de droits et de privilèges d'accès.
      d. La création, la suppression ou la modification de mots de passe.

   ii. Les renseignements/biens ci-dessous doivent être consignés pour chacun des événements ci-dessus :

      a. Type d'activité
      b. Code d'utilisateur
      c. Date et heure;
      d. Code du dispositif.

Les enregistrements des comptes rendus doivent être archivés à un endroit qui permet au gestionnaire du système d'information d'obtenir un compte rendu imprimé de chaque activité choisie. Il faut

également prévoir un endroit qui se prête à l'impression des enregistrements sous forme lisible. Les utilisateurs qui n'ont aucun « besoin de savoir » ne doivent pas avoir accès aux enregistrements relatifs à la sécurité.

Si le système d'exploitation ne permet pas d'offrir cette fonction, le matériel doit être protégé par des moyens physiques lorsqu'il n'est pas utilisé (p. ex. dans un endroit fermé à clé ou en enlevant le disque dur pour le mettre sous clé)

g. **Intégrité et disponibilité :** Les mesures suivantes doivent être mises en œuvre:

i. Assurer une protection générale contre des accidents prévisibles, des incidents et des problèmes connus et répétés (p. ex. virus et fluctuations de la tension de l'alimentation en électricité);
ii. Plan opérationnels d'urgence précis;
iii. Sauvegarde et archivage sur place des données; et
iv. Logiciel antivirus (installation et mise à jour d'un logiciel antivirus acceptable, conforme aux normes de l'industrie).

h. **Messages d'ouverture de session :** Autant que possible, un message d'ouverture de session doit fournir un résumé des conditions d'utilisation du système d'information, afin que l'on puisse s'en servir pour intenter des poursuites en cas d'infraction. Voici un exemple de message d'ouverture de session: « L'accès non autorisé à cet ordinateur peut constituer un acte criminel. »

i. **Terminaux laissés sans surveillance :** Les utilisateurs autorisés doivent être déconnectés automatiquement du système lorsque les terminaux n'ont pas été utilisés pendant une période préétablie. À titre de solution de rechange, le terminal doit activer un écran de veille protégé par un mot de passe après 15 minutes d'inactivité, afin d'empêcher un intrus d'utiliser un terminal laissé sans surveillance.

j. **Connexions Internet** : Les ordinateurs ne doivent pas être reliés directement à Internet s'ils ne sont pas protégés par un pare-feu (un logiciel pare-feu personnel est le minimum exigé).

k. **Disposition** : Avant d'éliminer un support de données informatiques (p. ex. des disquettes), un produit d'effacement des données doit être utilisé afin d'écraser les données. Ce processus est plus sûr que le simple efficacement des fichiers.

Annexe A

L'entrepreneur / Le sous-traitant étranger destinataire doit effectuer les vérifications suivantes de tous ses employés qui auront **l'accès à des lieux à accès restreint au Canada et/ou l'accès à des renseignements/biens de niveau CANADA PROTÉGÉS A**:

a) Vérification d'identité :
   i. Copies de deux pièces d'identité valides émises par le gouvernement, dont l'une avec photo

ii. Nom de famille
iii. Prénom(s) – souligner ou encercler le prénom usuel
iv. Nom de famille à la naissance
v. Autres noms utilisés (alias)
vi. Changements de noms
    1. Indiquer le nom d'origine (avant le changement) et le nouveau nom, l'endroit où le changement a été effectué et l'institution qui a traité la demande.
vii. Sexe
viii. Date de naissance
ix. Lieu de naissance (ville, province/état/région et pays)
x. Citoyenneté(s)
xi. État matrimonial/union de fait
    1. Situation actuelle (marié, union de fait, séparé, veuf, divorcé, célibataire)
    2. Conjoint(s) actuel(s) (s'il y a lieu
        a. Nom de famille
        b. Prénom complet – souligner ou encercler le prénom usuel
        c. Date et durée du mariage/de l'union de fait
        d. Date de naissance
        e. Nom de famille à la naissance
        f. Lieu de naissance (ville, province/état/région et pays)
        g. Citoyenneté

b) Vérification du lieu de résidence :
    i. Historique des lieux où vous avez habité au cours des cinq (5) dernières années, du plus récent au plus ancien, sans écart au niveau des dates.
        1. Numéro d'appartement, numéro de porte, nom de la rue, ville, province ou état, code postal ou zip, pays, durée de la période d'habitation.

c) Vérification des titres professionnels :
    i. Établissements d'enseignement fréquentés et dates correspondantes.

d) Vérification de l'historique d'emploi :
    i. Historique des cinq (5) dernières années d'emploi, à partir de l'emploi le plus récent, sans écart au niveau des dates.
    ii. Trois (3) vérifications des références d'emploi menées au cours des cinq (5) dernières années.

e) Vérification des antécédents criminels :
    i. Document(s) décrivant l'ensemble des condamnations criminelles au cours des cinq (5) dernières années, à l'intérieur et à l'extérieur du pays de résidence du candidat.

f) Rapport de la vérification du crédit :
    i. Rapport de la vérification du crédit si disponible.