ANNEX E - SUPPLY CHAIN SECURITY INFORMATION ASSESSMENT PROCESS

Introduction

Bidders must submit specific information regarding each component of their proposed Solution's supply chain. This information is referred to as *Supply Chain Security Information (SCSI)*. This information will be used by Canada to assess whether, in its opinion, a bidder's proposed supply chain creates the possibility that the bidder's proposed Solution could compromise or be used to compromise the security integrity of Canada's equipment, firmware, software, systems or information in accordance with the process found in this Annex. This assessment is referred to as the SCSI Assessment Process.

Bidders must provide their SCSI for a solution that is hosted within Canada's technical environment (refer to Appendix A to Annex E – Conceptual View of Technical Environment)

Definitions

The following words and expressions used with respect to SCI Process have the following meanings:

a. "**OEM Name**" means the name of the original equipment manufacturer (OEM) of the product that is being ordered.

b. "**OEM DUNS Number**" means the Data Universal Numbering System (DUNS). It is a unique nine-digit number assigned to each physical location of a business. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.

c. **Product Name** means the OEM's name for the product;

d. **Model Number** means the OEM's model and/or version number of the product.

e. **Vulnerability Information** means the information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers **separated by semi-colons (;)**.
If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and provide this information to the Canadian Centre for Cyber Security. If this is the case for a particular product, enter "see attached information" in the relevant field(s).

f. **Supplier Name** means the name of the supplier (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product that is being ordered. This includes any business entity involved in producing products or services to help complete the bidding requirements.

g. **Supplier DUNS Number** is already explained above.

h. **Supplier URL** means the URL of the supplier's webpage for the product.

i. **Ownership** means the top 5, by percentage, owners of the OEM or Supplier. The names provided for owners should be those found in ownership documents for the company in question.

j. **Investors** means the top 5, by percentage, investor in the OEM or Supplier. The names provided for owners should be those found in investment documents for the company in question.

k. **Executives** means the executives and members of the board of directors for the company in question.

l. **Country / Nationality** means the country which an individual listed has their primary nationality or the country in which a corporate entity is registered.

m. **Corporate website link** means for each of OEM or Supplier name, Ownership, Investors, and Executives listed above provide a URI / URL to the information that supports the claims listed in each of the fields.

n. "**Supply Chain Security Information**" means any information that Canada requires a Bidder or Contractor to submit to conduct a complete security assessment of the SCSI as a part of the SCSI Assessment process.

Supply Chain Security Information Form Submission Requirements

Bidders must provide the following information by the bid closing date (see Part 2 – Bidder Instructions, Article 2.2 – Submission of Bids):

a. **IT Product List:** Bidders must identify the Products over which Canada's Data would be transmitted and/or on which Canada's Data would be stored, or that would be used and/or installed by the Bidder or any of its subcontractors to perform any part of the Work, together with the following information regarding each Product:

   i. OEM Name;

   ii. OEM DUNS Number;

   iii. Product Name;

   iv. Model Number;

   v. Vulnerability Information;

Bidders are requested to provide the IT Product information for their proposed Solution on Page *B – IT Product List*. Bidders are also requested to insert a separate row for each Product. Bidders are requested not to repeat multiple iterations of the same Product (e.g. if the serial number and/or color is the only difference between two products, they are considered the same Product within the confines of the SCI Assessment Process).

b. **Ownership Information**: "It is only necessary to fill out entries in ""C- Ownership Information"" if a DUNS number cannot be supplied for the OEM and/or supplier.

   i. Supplier Name;

   ii. Supplier DUNS Number;

   iii. Supplier URL;

   iv. Ownership;

   v. Investors;

   vi. Executives;

   vii. Country / Nationality;

viii. Corporate website link.

Assessment of Supply Chain Security Information

a. Canada will assess whether, in its opinion, the SCSI creates the possibility that the Bidder's solution could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information.

b. In conducting its assessment:

   i. Canada may request from the Bidder any additional information that Canada requires to conduct a complete security assessment of the SCSI. The Bidder will have 2 working days (or a longer period if specified in writing by Canada) to provide the necessary information to Canada.

   ii. Canada may use any government resources to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is included in the bid or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of the SCSI.

c. If, in Canada's opinion, there is a possibility that any aspect of the SCSI, if used by Canada, could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information:

   i. Canada will notify the Bidder in writing (sent by email) and identify which aspect(s) of the Bidder's SCSI is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Bidder regarding its concerns will be determined based on the nature of the concerns. In some situations, for reasons of national security, it may not be possible for Canada to provide further information to the Bidder; therefore, in some circumstances, the Bidder will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the Bidder's SCSI. With respect to any concerns, Canada may, in its discretion, identify a potential mitigation measure that the Bidder would be required to implement with respect to any portion of the SCSI if awarded a contract.

   ii. Upon receipt of Canada's written notice, the Bidder will be given one opportunity to submit a revised SCSI. If Canada has identified a potential mitigation measure that the supplier would be required to implement if awarded a contract, the Bidder must confirm in its revised SCSI whether or not it agrees that any awarded contract will contain additional commitments relating to those mitigation conditions. The revised SCSI must be submitted within the **10 calendar days** following the day on which Canada's written notification is sent to the Bidder (or a longer period specified in writing by the Contracting Authority).

d. If the Bidder submits a revised SCSI within the allotted time, Canada will perform a second assessment. If in Canada's opinion, there is a possibility that any aspect of the Bidder's revised SCSI could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, the Bidder will be provided with the same type of notice described under paragraph c), above. Any further opportunities to revise the SCSI will be entirely at the discretion of Canada and all SCSI respondents will be offered the same opportunity. By participating in this process, the Bidder acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. As a result:

i. qualification pursuant to this SCSI Assessment Process does not constitute an approval that the products or other information included as part of the SCSI will meet the requirements of the resulting contract;

ii. qualification pursuant to this SCSI Assessment Process does not mean that the same or similar SCSI will be assessed in the same way for future requirements;

iii. at any time during this bid solicitation process, Canada may advise a Bidder that some aspect(s) of its SCSI has become the subject of security concerns. At that point, Canada will notify the Bidder and provide the Bidder with an opportunity to revise its SCSI, using the process described above; and,

iv. during the performance of any contract resulting from this bid solicitation, if Canada has concerns regarding certain products, designs or subcontractors originally included in the SCSI, the terms and conditions of that contract will govern the process for addressing those concerns.

Upon completion of the SCSI Integrity Assessment, Bidders will be notified of the results through the Contracting Authority.

Tab A – SCSI Form 2 Cover

Supply Chain Security Information (SCSI)
Vendor Submission Form

PART A - BIDDER INFORMATION	
Procurement Name:	
Date submitted:	
Solicitation Number:	
Bidder Name:	
Bidder DUNS Number:	

PART B - PRODUCT LIST
CLICK HERE TO ADD ITEMS +

PART C - OWNERSHIP INFORMATION
CLICK HERE TO ADD ITEMS +

Please save this form only in Excel format before submitting. Please do not use other formats.

Tab B – IT PRODUCT LIST

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Supplier Name	Supplier DUNS Numbe	Supplier URL	Additional Information
1										
2										
3										
4										
5										

Tab C – Ownership Information

Item	OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
1						
2						
3						

Insert as Appendix A to Annex E – Conceptual View of Technical Environment, the following: