PART 1 – General Information

1.1.1 Canada will require the top ranked responsive bidder per radio stream, as determined by Canada following bid evaluation, to comply with the Supply Chain Integrity (SCI) Assessment specified below. To be awarded a standing offer, the Bidder must successfully complete the SCI and not be disqualified. If the top-ranked Bidder does not meet the SCI Assessment, then the second-ranked Bidder will be requested to comply with the SCI Assessment. If the second-ranked Bidder does not comply with the SCI Assessment, then the third-ranked Bidder will be requested to comply with the SCI Assessment. If none of these Bidders meet these requirements, then Canada may, but will have no obligation to, continue down the list of responsive Bidders until one responsive Bidder meets the SCI Assessment. A responsive Bidder must meet SCI Assessment to be eligible for standing offer award.

1.1.2 **Supply Chain Integrity (SCI) Assessment:**

1.1.2.1 The Supply Chain Integrity (SCI) Assessment will apply to this procurement. Responsive Bidders must provide the information specified at **Annex I – Supply Chain Security Information (SCSI) to Canada upon request**. SCI is an important corporate requirement. Challenged by an increasingly complex cyber threat environment, Canada is committed to applying enhanced security process and standing offer clauses to the acquisition of both products and services. The purpose of the SCI Assessment is to ensure that all proposed sub-contractors, products, equipment, software, firmware and services that are procured by PSPC meet the required security and supply chain standards as determined by Canada.

1.1.2.2 Canada will assess information submitted by the Bidder in accordance with **Annex I – Supply Chain Security Information**..

PART 6 – Standing Offer and Resulting Contract Clauses

1.2 **On-going Supply Chain Integrity Process**

A. Supply **Chain Integrity Process:** The Parties acknowledge that a Supply Chain Integrity Process assessment was a key component of the procurement process that resulted in the award of this Standing Offer. In connection with that assessment process, Canada assessed the Offeror's Supply Chain Security Information (SCSI) without identifying any security concerns. The following SCSI was submitted: an IT Product List; and

B. a list of subcontractors;

This SCI is included as part of the SCI Annex I. The Parties also acknowledge that on-going assessment of SCSI will be required throughout the Standing Offer Period. This Article governs that process.

1.2.1 **Assessment of New SCSI:** During the Standing Offer Period, the Offeror may need to modify the SCSI information contained in Annex I. In that regard:

1.2.1.1 The Offeror, starting at standing offer award, must revise its SCSI at least once a month to show all changes made, as well as all deletions and additions to the SCSI that affect the services under the Standing Offer (including Products deployed by its subcontractors) during that period; the list must be marked to show the changes made during the applicable period. If no changes have been made during the reporting month, the Offeror must advise the Contracting Authority in writing that the existing list is unchanged.

1.2.1.2 The Offeror agrees that, during the Standing Offeror Period, it will periodically (at least once a year) provide the Contracting Authority with updates regarding upcoming new Products that it anticipates deploying in the Work (for example, as it develops its "technology roadmap" or similar plans). This will allow Canada to assess those Products in advance so that any security concerns can be identified prior to the Products being deployed in connection with the services being delivered under the Standing Offer. Canada will endeavour to assess proposed new Products within 30 calendar days, although lengthier lists of Products may take additional time.

1.2.1.3 Canada reserves the right to conduct a complete, independent security assessment of all new SCSI. The Offeror must, if requested by the Contracting Authority, provide any information that Canada requires to perform its assessment.

1.2.1.4 Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is provided by the Offeror or comes from another source, that Canada considers advisable to conduct a comprehensive assessment of any proposed new SCSI.

1.2.2 Identification **of New Security Vulnerabilities in SCSI already assessed by Canada:**

1.2.2.1 The Offeror must provide to Canada timely information about any vulnerabilities of which it becomes aware in performing the Work, including any weakness, or design deficiency, identified in any Product used to deliver services that would allow an unauthorized individual to compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications it hosts.

1.2.2.2 The Offeror acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified and, that being the case, new security vulnerabilities may be identified in SCSI that have already been the subject of an SCSI assessment and assessed without security concerns by Canada, either during the procurement process or later during the Standing Offer Period.

1.2.3 Addressing **Security Concerns:**

1.2.3.1 If Canada notifies the Offeror of security concerns regarding a Product that has not yet been deployed, the Offeror agrees not to deploy it in connection with this Standing Offer without the written consent of the Contracting Authority.

1.2.3.2 At any time during the Standing Offer Period, if Canada notifies the Offeror that, in Canada's opinion, there is a Product that is being used in the Offeror's solution (including use by a subcontractor) that has been assessed as having the potential to compromise or be used to compromise the security of

Canada's equipment, firmware, software, systems or information, then the Offeror must:

C. provide Canada with any further information requested by the Contracting Authority so that Canada may perform a complete assessment;

D. if requested by the Contracting Authority, propose a mitigation plan (including a schedule), within 10 business days, such as migration to an alternative Product. The Contracting Authority will notify the Offeror in writing if Canada approves the mitigation plan, or will otherwise provide comments about concerns or deficiencies with the mitigation plan; and

E. implement the mitigation plan approved by Canada.

F. This process applies both to new Products and to Products that were already assessed pursuant to the Supply Chain Integrity Process assessment by Canada, but for which new security vulnerabilities have since been identified.

1.2.3.3 Despite the previous Sub-article, if Canada determines in its discretion that the identified security concern represents a threat to national security that is both serious and imminent, the Contracting Authority may require that the Offeror immediately cease deploying the identified Product(s) in the Work. For Products that have already been deployed, the Offeror must identify and/or remove (as required by the Contracting Authority) the Product(s) from the Work according to a schedule determined by Canada. However, prior to making a final determination in this regard, Canada will provide the Offeror with the opportunity to make representations within 48 hours of receiving notice from the Contracting Authority. The Offeror may propose, for example, mitigation measures for Canada's consideration. Canada will then make a final determination.

1.2.4 **Cost** Implications**:**

1.2.4.1 Any cost implications related to a demand by Canada to cease deploying or to remove a particular Product or Products will be considered and negotiated in good faith by the Parties on a case-by-case basis and may be the subject of a Standing Offer Amendment, However, despite any such negotiations, the Offeror must cease deploying and/or remove the Product(s) as required by Canada. The negotiations will then continue separately. The Parties agree that, at a minimum, the following factors will be considered in their negotiations, as applicable:

G. with respect to Products already assessed without security concerns by Canada pursuant to an SCSI assessment, evidence from the Offeror of how long it has owned the Product;

H. with respect to new Products, whether or not the Offeror was reasonably able to provide advance notice to Canada regarding the use of the new Product in connection with the Work;

I. evidence from the Offeror of how much it paid for the Product, together with any amount that the Offeror has pre-paid or committed to pay with respect to maintenance and support of that Product;

J. the normal useful life of the Product;

K. any "end of life" or other announcements from the manufacturer of the Product indicating that the Product is or will no longer be supported;

L. the normal useful life of the proposed replacement Product;

M. the time remaining in the Standing Offer Period;

N. whether or not the existing Product or the replacement Product is or will be used exclusively for Canada or whether the Product is also used to provide services to other customers of the Offeror or its subcontractors;

O. whether or not the Product being replaced can be redeployed to other customers;

P. any training required for Offeror personnel with respect to the installation, configuration and maintenance of the replacement Products, provided the Offeror can demonstrate that its personnel would not otherwise require that training;

Q. any developments costs required for the Offeror to integrate the replacement Products into operations, administration and management systems, if the replacement Products are Products not otherwise deployed anywhere in connection with the Work; and

R. the impact of the change on Canada, including the number and type of resources required and the time involved in the migration.

1.2.4.2 Additionally, if requested by the Contracting Authority, the Offeror must submit a detailed cost breakdown, once any work to address a security concern identified under this Article has been completed. The cost breakdown must contain an itemized list of all applicable cost elements related to the work required by the Contracting Authority and must be signed and certified as accurate by the Offeror's most senior financial officer, unless stated otherwise in writing by the Contracting Authority. Canada must consider the supporting information to be sufficiently detailed for each cost element to allow for a complete audit. In no case will any reimbursement of any expenses of the Offeror (or any of its subcontractors) exceed the demonstrated out-of-pocket expenses directly attributable to Canada's requirement to cease deploying or to remove a particular Product or Products.

1.2.4.3 Despite the other provisions of this Article, if the Offeror or any of its subcontractors deploys new Products that Canada has already indicated to the Offeror are the subject of security concerns in the context of the Work, Canada may require that the Offeror or any of its subcontractors immediately cease deploying or remove that Product. In such cases, any costs associated with complying with Canada's requirement will be borne by the Offeror and/or subcontractor, as negotiated between them. Canada will not be responsible for any such costs.

1.2.5 General:

1.2.5.1 The process described in this Article may apply to a single Product, to a set of Products, or to all Products manufactured or distributed by a particular supplier.

1.2.5.2 The process described in this Article also applies to subcontractors. With respect to cost implications, Canada acknowledges that the cost considerations with respect to concerns about subcontractors (as opposed to Products) may be different and may include factors such as the availability of other subcontractors to complete the work.

1.2.5.3 Any service levels that are not met due to a transition to a new Product or subcontractor required by Canada pursuant to this Article will not trigger a Service Credit, nor will a failure in this regard be taken into consideration for overall metric calculations, provided that the Offeror implements the necessary changes in accordance with the migration plan approved by Canada or proceeds immediately to implement Canada's requirements if Canada has determined that the threat to national security is both serious and imminent.

1.2.5.4 If the Offeror becomes aware that any subcontractor is deploying Products subject to security concerns in relation to the Work, the Offeror must immediately notify both the Contracting Authority and the Technical Authority and the Offeror must enforce the terms of its standing offer with its subcontractor.

1.2.5.5 Any determination made by Canada will constitute a decision with respect to a specific Product or subcontractor and its proposed use under this Standing Offer, and does not mean that the same Product or subcontractor would necessarily be assessed in the same way if proposed to be used for another purpose or in another context.