Purchasing Office / Bureau des achats:

Procurement and Vendor Relationships/
Acquisitions et relations avec les fournisseurs
180, rue Kent Street, 13th Floor/
13 ième étage
P.O. Box 9808, STN T CSC /
CP 9808, succursale T CSC
Ottawa, Ontario K1G 4A8

Challenge-Based Standing Offer - D'offres à Commandes par Défi

You are requested to sell to Her Majesty the Queen, in right of Canada, in accordance with the terms and conditions set out herein, referred to herein or attached hereto, the goods, services, and construction listed herein and on any attached sheets at the price or prices set out thereof.

Nous vous demandons de vendre à sa Majesté la Reine du Chef du Canada, aux conditions énoncées ou incluses par référence dans les présentes, et aux annexes ci-jointes, les biens, services et construction énumérés dans les présentes, et sur toute feuille ci-annexée, au(s) prix indiqué(s).

The Vendor/Firm hereby accepts/acknowledges this Standing Offer.

Le fournisseur/entrepreneur accepte le présent offer à commandes/en accuse réception

Signature

Date
2023-02-07

Vendor/Firm Name and address:
Raison sociale et adresse du fournisseur/de l'entrepreneur:

PBN : 830457206PG0001
TitanFile Inc.
1050 King St. W.
Toronto ON
M6K 0C7

Title – Sujet
Next Generation Litigation Software - Secure File Transfer Solution

Challenge-Based Standing Offer No. - No D'offres à Commandes par Défi
2BS-0-85236-B

Amendment No. - N° Modif	**Date**
1	February 01, 2023

Reference No. – N° de reference
P2P R109093

F.O.B. - F.A.B.
See Herein

GST/HST – TPS/TVH	**Duty – Droits**
See Herein	See Herein

Destination of Goods, Services, and Construction - Destination des biens, services et construction :
As per Individual Call-up

Invoices – Factures
As per Individual Call-up

Address Inquiries to - Adresser toutes questions à:
Michaela Criper– michaela.criper@canada.ca
613-462-9890

Total Estimated Call-Up Value – Coût total estimatif (taxes inc)	**Currency Type – Devise**
	CAD

For the Minister – Pour le Ministre

Currie, Andrea
Digitally signed by Currie, Andrea
Date: 2023.02.03 17:13:05 -05'00'

Signature Date

Andrea Currie | Manager
Internal and Digital Services Procurement (IDSP) | Services d'aquisitions internes et numériques (SAIN)
Enterprise IT Procurement (EITP) | Approvisionnement en TI pour l'entreprise (ATIE) Shared Services Canada
Shared Services Canada | Services partagés Canada

Amendment No. 1

Entire Agreement of the Parties

This Standing Offer constitutes and contains the entire understanding and agreement of the Parties respecting the subject matter hereof and cancels and supersedes any and all prior negotiations, correspondence, understandings, and agreements between the Parties, whether oral or written, regarding such subject matter.

No waiver, modification, or amendment of any provision of this Standing Offer shall be valid or effective unless made in writing referencing this Standing Offer and signed by a duly authorized officer of each Party.

Table of Contents

STANDING OFFER AND RESULTING CONTRACT CLAUSES

The following terms and conditions are intended to form the basis of this Challenge-Based Standing Offer (Standing Offer).

No modification to the Standing Offer terms and conditions included in the Offeror's Offer, statements implying that the Offer is conditional on modification to these Standing Offer terms and conditions (including all documents incorporated into the Standing Offer by reference), or terms and conditions that purport to supersede these Standing Offer terms and conditions will apply to the Standing Offer, even though the Offer may become part of the Standing Offer.

No alternative licensing conditions for licensed software included in the Offeror's Offer, or any terms and conditions in the Offeror's Offer with respect to limitations on liability, or any terms and conditions incorporated into the Offeror's Offer by reference, will apply to the Standing Offer even though the Offer may become part of the Standing Offer. Additional terms and conditions; including alternative licensing conditions for licensed software approved by Canada (if any), are only binding on Canada if they have been included in the Standing Offer at the paragraph entitled *Additional Terms and Conditions - Approved by Canada*.

SECTION 1 STANDING OFFER

1.1 Offer

The Offeror offers to fulfil the Requirement(s) in accordance with Attachment A - Statement of Challenge.

1.2 Series of Standing Offers

The Offeror acknowledges that this Standing Offer was awarded as a result of the Challenge-Based Standing Offer Solicitation (CBSOS) issued by Canada on October 27, 2021, under Solicitation No. 2BS-0-85236/B.

The award of this Standing Offer begins Work Segment 2 of the overall Secure File Transfer initiative described in Attachment A - Statement of Challenge.

1.3. Solution(s) to be Deployed (Work Segment 2)

Following the completion of Work Segment 1 (Proof of Concept), Canada has; in a timely and equal manner, informed all Offerors in the procurement ecosystem of which Solution(s) is to remain available for Call-up Allocation, i.e., Solution(s) to be deployed, and in doing so exercised its right in its sole discretion to award this Standing Offer.

1.4 Work Segments (WS) - Standing Offer Call-ups

The following WSs and associated Call-ups are available to Canada under this Standing Offer.

a) **WS 2 Call-ups:**

- Deployment of the Operational Solution (User or Entity Based)

b) **Additional Call-ups Available to Canada:**

- Call-ups - Solution Improvements
- Call-ups - Professional Services
- Call-ups - Virtual Training Services
- Call-ups - Catch-All

The prices for Call-ups exercised 24 months after the date of Standing Offer award, and at the request of the Offeror, will be adjusted in accordance with the paragraph entitled *Price Adjustment Mechanism*.

1.4.1 WS 2 Call-ups - Deployment of the Operational Solution (User or Entity Based)

The Standing Offer Authority may issue WS 2 Call-ups to require the Offeror to deploy the Operational Solution, in accordance with the terms and conditions of this Standing Offer, including Attachment A - Statement of Challenge, and in accordance with the prices set out in Attachment B - Basis of Payment.

Note: WS 2 Call-ups may include Call-ups for:

- Deployment of the Operational Solution (User or Entity Based)
- Secure File Transfer - Annual Subscription Licenses (User or Entity Based)
- Additional User Licenses

While the decision to issue WS 2 Call-ups is entirely within Canada's discretion, if Canada chooses to issue WS 2 Call-ups, it will do so in accordance with the *Call-up Allocation Method (CAM)*, refer to section 1.6.

Canada anticipates selecting 1 Offeror to proceed with the Deployment of the Operational Solution for the Department of Justice. However, Canada may at its discretion, issue WS 2 Call-ups to other Offerors at any time prior to the expiry date of the Standing Offer.

1.4.2 Deployment on Additional Client's Operational Environments

Shared Services Canada (SSC) is a federal government department that acts as a shared services organization. SSC will use the Solution(s) resulting from the CBSOS Solicitation No. 2BS-0-85236/B issued on October 27, 2021, to provide a Solution(s) to one or more of its Clients. The initial lead client will be the Department of Justice, and SSC may select other Clients to use the Solution(s), for example, for further testing of the Solution.

SSC's "Clients" include SSC itself, those government institutions for whom SSC's services are mandatory, and those other organizations for whom SSC's services are optional and that choose to use those services from time to time. In addition to the Government of Canada, SSC may also serve a government of a province or municipality in Canada, a Canadian aid agency, a public health organization, an intergovernmental organization, or a foreign government.

In deploying the Solution for additional Clients, there are potential "economies of scale" that may be realized, and that may reduce the Offeror's costs of performing the Work; consequently, a "price reduction" of the prices set out Attachment B - Basis of Payment, is a factor considered by Canada in its decision to issue WS 2 Call-ups - Deployment of the Operational Solution.

The Offeror acknowledges that Canada, prior to exercising WS 2 Call-ups - Deployment of the Operational Solution, may request a price reduction to the prices set out in Attachment B - Basis of Payment, based on economies of scale. The Standing Offering Authority may request the Offeror submit a price breakdown showing, if applicable, the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, markup, and any other supporting documentation.

For administrative purposes only, the Technical Authority, and Offeror's Representative under WS 2, will be determined by SSC's Client and the Offeror. The responsibilities of those Authorities, as specified under the Standing Offer, are transferred to the Authorities listed in the WS 2 Call-up Instrument.

For performance evaluation purposes, SSC's Clients will provide an annual usage report to the Standing Offering Authority specified herein, to summarize the usage, value, invoiced amounts, and lessons learned under their Standing Offer Call-ups.

1.4.3 Call-ups - Solution Improvements

Where the technological context renders available technological, administrative, commercial, or other types of "improvements" to the Solution that better resolve the problem(s) described in Attachment A - Statement of Challenge, the Standing Offer Authority may issue Call-ups - Solution Improvements to require the Offeror to provide those improvements in accordance with the terms and conditions of this Standing Offer including Attachment A - Statement of Challenge, and in accordance with the paragraph entitled *Basis of Payment - Solution Improvements*.

1.4.4 Call-ups - Professional Services

The Standing Offer Authority may issue Call-ups - Professional Services to require the Offeror to provide the Professional Services listed in Attachment A - Statement of Challenge, and in accordance with the prices set out in Attachment B - Basis of Payment.

1.4.4.1 SACC M3020C (2016-01-28): Status of Availability of Resources - Standing Offer

Is incorporated into the Standing Offer by reference.

1.4.5 Call-ups - Virtual Training Services

The Standing Offer Authority may issue Call-ups - Virtual Training Services to require the Offeror to provide the Virtual Training Services listed in Attachment A - Statement of Challenge, and in accordance with the prices set out in Attachment B - Basis of Payment.

1.4.6 Call-ups – Catch All

The Standing Offer Authority may issue Catch-All Call-ups to require the Offeror to provide any non-listed items that are intended, in their entirety or in part, for the Secure File Transfer project, in accordance with the terms and conditions of this Standing Offer including Attachment A - Statement of Challenge, and in accordance with the paragraph entitled *Basis of Payment: Call-up - Catch-All.*

1.5 Call-up Instrument and Procedures

1.5.1 Call-up Instrument

The Work will be authorized or confirmed by the Standing Offer Authority using form PWGSC-TPSGC 942 "Call-up Against a Standing Offer" or equivalent, which will contain at a minimum the following information:

- standing offer number;
- statement that incorporates the terms and conditions of the Standing Offer;
- description and unit price for each line item;
- total value of the call-up;
- point of delivery;
- confirmation that funds are available under section 32 of the Financial Administration Act;
- confirmation that the user is an Identified User under the Standing Offer with authority to enter into a contract.

1.5.2 Call-up Procedures

The Project Authority will provide the Offeror with a description of the Work to be performed under the Call-up; in accordance with the terms and conditions of the Standing Offer, including Attachment A - Statement of Challenge, in sufficient detail to enable the Offeror to establish a Firm Price for the Work.

The Offeror will submit a “Schedule of Costs” table with supporting details to the Project Authority in order to establish a Firm Price for the Work.

The Firm Price will be established in accordance with Attachment B - Basis of Payment, and where warranted and deemed appropriate by the Project Authority;

i) travel and living expenses as applicable will be calculated in accordance with current Treasury Board Travel Directives, with no allowance for profit or overhead; and where warranted and deemed appropriate by the Project Authority;

ii) other eligible costs not included in Attachment B - Basis of Payment, at direct cost with no allowance for profit or overhead.

The Work will be for a Firm Price; however, whenever the Work cannot be well defined, in lieu of a Firm Price, the Project Authority may pre-authorize a time rate payment, i.e., per diem rates, in accordance with the paragraph entitled *Professional Services* found in Attachment B - Basis of Payment, or in accordance with the applicable principles for price justification, found in SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services - Competitive Requirements, subsection 14 *Price justification*, as applicable.

The “Schedule of Costs” table and Firm Price are subject to negotiation between the Offeror and the Project Authority.

Authorization to proceed with the Work will be made by the issuance of a Call-up Instrument duly signed by the Standing Offer Authority and the Project Authority.

1.5.3 Call-up Limitations

Individual call-ups against this Standing Offer must not exceed $ 100,000.00 (Goods and Services Tax or Harmonized Sales Tax excluded).

1.7 Standing Offers Reporting – Standing Offer Holder

The Standing Offer Holder must compile and maintain records on its provision of goods, services or both to Canada under Call-ups resulting from the Standing Offer. Whether or not the Standing Offer Holder’s, Standing Offer usage reports are acceptable to Canada, is determined entirely within the discretion of Canada. If Canada determines that the Standing Offer Holder’s reports do not provide sufficient data, the Standing Offer Authority will, by sending a written notice to the Standing Offer Holder, request that the Standing Offer Holder correct their usage reports within any time specified in the notice.

The Standing Offer Holder must provide this data in accordance with the reporting requirements detailed herein. If no goods or services are provided during a given period, the Standing Offer Holder must still provide a "NIL" report. Canada reserves the right to change the "NIL" reporting procedure at any time.

The data must be submitted on an annual basis, no later than 15 calendar days after the anniversary date of the Standing Offer.

Failure to provide fully completed reports in accordance with the above instructions may result in the setting aside of the Standing Offer.

1.8 Challenge-Based Standing Offer Holders List - Refresh

Subsequent to the establishment of the Standing Offer Holders List, and throughout the period of the Standing Offer, Canada may, at its sole discretion, and at any point during the Standing Offer validity period, re-post the CBSOS Solicitation No. 2BS-0-85236/B issued on October 27, 2021 on Buyandsell.gc.ca .

This would permit additional Vendors to qualify and to be added to the Standing Offer Holders List, and to allow existing Standing Offer Holders to submit new Financial Offers to refresh their Standing Offer prices.

Offers will be subject to the same qualification requirements as those required in the original CBSOS, Solicitation No.: 2BS-0-85236/B issued on October 27, 2021.

(Note to Offerors: no existing Standing Offer Holder will be removed from the Standing Offer Holders List as a result of the addition of any newly qualified Offerors; however, the ranking of the Standing Offer Holders may be adjusted accordingly, as a result of the addition of newly qualified Offerors.)

1.9 Suspension or Set Aside of Standing Offer by Canada

Canada may, by sending written notice to the Offeror, exercise its right, in its sole discretion, to suspend or set aside the Standing Offer for the convenience of the Crown.

Suspension or set aside of the Standing Offer will not affect the right of Canada to pursue other remedies or measures that may be available. It will not, on its own, affect any Call-up entered into before the issuance of the notice. The Standing Offer Authority will however remove the Offeror from the list of Standing Offer Holders eligible to receive Call-ups under this Standing Offer. The Offeror will not be able to submit another Offer, and the Offeror will not be allowed to submit a new Offer for consideration until the requirement is re-competed.

1.10 Standard Clauses and Conditions

All clauses and conditions identified in the Standing Offer by number, date and title are set out in the Standard Acquisition Clauses and Conditions (SACC) Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada (PWGSC.)

1.10.1 General Conditions

The following General Condition is incorporated by reference.

SACC 2005 (2017-06-21), General Conditions - Standing Offers **-** Goods or Services, apply to and form part of this Standing Offer.

All references contained within the SACC 2005 (2017-06-21), General Conditions - Standing Offers - Goods or Services, or in any Call-up Instrument (PWGSC-TPSGC 942 “Call-up Against a Standing Offer”) or equivalent, to the Minister of Public Works and Government Services will be interpreted as a reference to the Minister of Digital Government presiding over SSC and all references to the department of Public Works and Government Services will be interpreted as a reference to SSC.

1.11 Security Requirements

Refer to Attachment A1 – Security Requirements for a detailed description of the Security Requirements.

1.12 Evolving Security Requirements (Evergreen)

As a result of the Standing Offer being perpetual, from time to time, SSC may amend any Security Requirement provision outlined in any part of the Standing Offer as a result of a policy notification, legislation, procedural or technological change. Any such change will not affect existing contracts in place prior to the date of change. Notification of such change will be sent to the Offer Holder via a generic email, and Canada will request the Offer Holder to endorse the proposed amendment.

Should an Offer Holder not agree with such modifications, and no longer wishes to be considered for requirements raised under the Standing Offer as a result of the changes, the Offer Holder will notify the Standing Offer Authority and this Offer Holder will no longer be on the list of Standing Offer Holders.

1.13 Cloud Security Requirements

Refer to Attachment A2 – Cloud Security Requirements for a detailed description of the Cloud Security Requirements.

1.14 Evolving Cloud Security Requirements (Evergreen)

As a result of the Standing Offer being perpetual, from time to time, SSC may amend any Cloud Security Requirement provision outlined in any part of the Standing Offer as a result of a policy notification, legislation, procedural or technological change. Any such change will not affect existing contracts in place prior to the date of change. Notification of such change will be sent to the Offer Holder via a generic email, and Canada will request the Offer Holder to endorse the proposed amendment.

Should an Offer Holder not agree with such modifications, and no longer wishes to be considered for requirements raised under the Standing Offer as a result of the changes, the Offer Holder will notify the Standing Offer Authority and this Offer Holder will no longer be on the list of Standing Offer Holders.

1.15 Supply Chain Integrity (SCI) Process

1.15.1 On-going Supply Chain Integrity Process

(Note to Offerors: Canada has determined that a thorough assessment of the supply chain associated with the goods and services to be acquired under this Standing Offer is critical to Canada's national security. In order to be issued any post WS 1 Proof of Concept Call-ups, the Offeror must complete the Supply Chain Security Information (SCSI) assessment process without Canada identifying any security concerns. In connection with that assessment process, the Offeror must provide to the Standing Offer Authority a completed SCSI Submission Form within the specified time frame within which to comply with the Standing Offer Authority's request.)

(a) Supply Chain Integrity Process

The Parties acknowledge that a Supply Chain Integrity Process assessment is a key component of this Standing Offer. In connection with that assessment process, Canada will assess the Offeror's Supply Chain Security Information (SCSI).

This Offeror's SCSI is included as Attachment C – SCSI Vendor Submission Form. The Parties also acknowledge that security is a critical consideration for Canada with respect to this Standing Offer and that on-going assessment of SCSI will be required throughout the Standing Offer Period. These following provisions govern that process.

(b) Assessment of New SCSI

During the Standing Offer Period, the Offeror may need to modify the SCSI information contained in Attachment C. In that regard:

(i) 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 Work 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 Standing Offer Authority in writing that the existing list is unchanged;

(ii) the Offeror agrees that, during the Standing Offer Period, it will periodically (at least once a year) provide the Standing Offer 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 Work 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;

(iii) Canada reserves the right to conduct a complete, independent security assessment of all new SCSI. The Offeror must, if requested by the Standing Offer Authority, provide any information that Canada requires to perform its assessment; and

(iv) 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.

(c) Identification of New Security Vulnerabilities

(i) 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.

(ii) 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.

(d) Addressing Security Concerns

(i) 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 Standing Offer Authority.

(ii) 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:

- provide Canada with any further information requested by the Standing Offer Authority so that Canada may perform a complete assessment;
- if requested by the Standing Offer Authority, propose a mitigation plan (including a schedule), within 10 FGWDs, such as migration to an alternative Product. The Standing Offer 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
- implement the mitigation plan approved by Canada.

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.

(iii) Despite the previous provision, if Canada determines in its discretion that the identified security concern represents a threat to national security that is both serious and imminent, the Standing Offer 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 Standing Offer 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 Standing Offer Authority. The Offeror may propose, for example, mitigation measures for Canada's consideration. Canada will then make a final determination.

(e) Cost Implications

(i) 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 or Contract 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:

- 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;
- 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;
- 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;
- the normal useful life of the Product;
- any "end of life" or other announcements from the manufacturer of the Product indicating that the Product is or will no longer be supported;
- the normal useful life of the proposed replacement Product;
- the time remaining in the Standing Offer or Contract Period;
- 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;
- whether or not the Product being replaced can be redeployed to other customers;
- 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;
- 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
- the impact of the change on Canada, including the number and type of resources required and the time involved in the migration.

(ii) Additionally, if requested by the Standing Offer Authority, the Offeror must submit a detailed cost breakdown, once any work to address a security concern identified under this provision has been completed. The cost breakdown must contain an itemized list of

all applicable cost elements related to the Work required by the Standing Offer Authority and must be signed and certified as accurate by the Offeror's most senior financial officer, unless stated otherwise in writing by the Standing Offer 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.

(iii) Despite the other provisions herein, 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 Offeror and/or Subcontractor, as negotiated between them. Canada will not be responsible for any such costs.

(f) General

The processes described in these provisions may apply to a single Product, to a set of Products, or to all Products manufactured or distributed by a particular supplier.

The processes described in these provisions also apply 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.

Any service levels (if applicable) that are not met due to a transition to a new Product or Subcontractor required by Canada pursuant to these provisions 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.

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 Standing Offer Authority and the Technical Authority and the Offeror must enforce the terms of its contractual agreement with its Subcontractor.

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.

1.15.2 Change of Control

(a) At any time during the Standing Offer Period, if requested by the Standing Offer Authority, the Offeror must provide to Canada:

(i) an organization chart for the Offeror showing all related corporations and partnerships; for the purposes of this sub-provision, a corporation or partnership will be considered related to another entity if:

- they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;
- the entities have now or in the two years before the request for the information had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or
- the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

(ii) a list of all the Offeror's shareholders; if the Offeror is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; with respect to any publicly traded corporation, Canada anticipates that the circumstances in which it would require a complete list of shareholders would be unusual and that any request from Canada for a list of a publicly traded corporation's shareholders would normally be limited to a list of those shareholders who hold at least 1% of the voting shares;

(iii) a list of all the Offeror's directors and officers, together with each individual's home address, date of birth, birthplace, and citizenship(s); if the Offeror is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; and any other information related to ownership and control that may be requested by Canada.

(b) If requested by the Standing Offer Authority, the Offeror must provide this information regarding its Subcontractors as well. However, if a Subcontractor considers this information to

be confidential, the Offeror may meet its obligation by having the Subcontractor submit the information directly to the Standing Offer Authority.

(c) The Offeror must notify the Standing Offer Authority in writing of:

(i) any change of control in the Offeror itself;

(ii) any change of control in any parent corporation or parent partnership of the Offeror, up to the ultimate owner; and

(iii) any change of control in any Subcontractor performing any part of the Work (including any change of control in any parent corporation or parent partnership of the Subcontractor, up to the ultimate owner).

The Offeror must provide this notice by no later than 10 FGWDs after any change of control takes place (or, in the case of a Subcontractor, within 15 FGWDs after any change of control takes place). Where possible, Canada requests that the Offeror provide advance notice of any proposed change of control transaction.

(d) In this provision, a "change of control" includes but is not limited to a direct or indirect change in the effective control of the corporation or partnership, whether resulting from a sale, encumbrance, or other disposition of the shares (or any form of partnership units) by any other means. In the case of a joint venture Offeror or Subcontractor, this applies to a change of control of any of the joint venture's corporate or partnership members. In the case of an Offeror or Subcontractor that is a partnership or limited partnership, this requirement also applies to any corporation or limited partnership that is a partner.

(e) If Canada determines in its sole discretion that a change of control affecting the Offeror (either in the Offeror itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada may terminate the Standing Offer or Contract on a "no-fault" basis by providing notice to the insert Offeror within 90 days of receiving the notice from the Offeror regarding the change of control. Canada will not be required to provide its reasons for terminating the Standing Offer or Contract in relation to the change of control, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security.

(f) If Canada determines in its sole discretion that a change of control affecting a Subcontractor (either in the Subcontractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada will notify the Offeror in writing of its determination. Canada will not be required to provide the reasons for its determination, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security.

The Offeror must, within 90 days of receiving Canada's determination, arrange for another Subcontractor, acceptable to Canada, to perform the portion of the Work being performed by the existing Subcontractor (or the Offeror must perform this portion of the Work itself). If the Offeror fails to do so within this time period, Canada will be entitled to terminate the Standing Offer or Contract on a "no-fault" basis by providing notice to the Offeror within 180 days of receiving the original notice from the Offeror regarding the change of control.

(g) In this provision, termination on a "no-fault" basis means that neither party will be liable to the other in connection with the change of control or the resulting termination, and Canada will only be responsible for paying for those services received up to the effective date of the termination.

(h) Despite the foregoing, Canada's right to terminate on a "no-fault" basis will not apply to circumstances in which there is an internal reorganization that does not affect the ownership of the ultimate parent corporation or parent partnership of the Offeror or Subcontractor, as the case may be; that is, Canada does not have a right to terminate the Standing Offer or Contract pursuant to this provision where the Offeror or Subcontractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner. However, in any such case, the notice requirements of this provision still apply.

1.15.3 Subcontracting

(a) Despite the General Conditions, none of the Work may be subcontracted (even to an affiliate of the Offeror) unless the Standing Offer Authority has first consented in writing. In order to seek the Standing Offer Authority's consent, the Offeror must provide the following information:

- the name of the Subcontractor;
- the portion of the Work to be performed by the Subcontractor;
- the Designated Organization Screening or the Facility Security Clearance (FSC) level of the Subcontractor;
- the date of birth, the full name and the security clearance status of individuals employed by the Subcontractor who will require access to Canada's facilities;
- completed sub-SRCL signed by the Offeror's Company Security Officer for CISD completion; and
- any other information required by the Standing Offer Authority.

(b) For the purposes of this provision, a “Subcontractor” does not include a supplier who deals with the Offeror at arm's length whose only role is to provide telecommunications or other equipment or software that will be used by the Offeror to provide services, including if the equipment will be installed in the backbone or infrastructure of the Offeror or Contractor.

1.16 Data Ownership and Sovereignty

The Parties agree that neither the operation of the Solution nor the provision of Operational Support and Maintenance Services (if applicable) for the Solution, requires the Offeror at any time to access the content transmitted by Canada using the Solution. The Offeror acknowledges that:

(a) it, its employees, representatives, and agents are prohibited from accessing the content transmitted by the Solution at any time without the written consent of the Standing Offer Authority; and

(b) it is prohibited from permitting any third party to access the content transmitted by the Solution at any time without the written consent of the Standing Offer Authority.

The Offeror agrees that, although it may access the Solution remotely, it must do so only from locations within Canada and the Offeror agrees to segregate its network or access to its network in all ways required in order to ensure that no person outside the geographic boundaries of Canada is capable of accessing the Solution remotely using the Offeror’s infrastructure. The Offeror acknowledges that Canada may audit compliance with this paragraph and agrees to provide access to its premises and systems during normal business hours to allow Canada or its representatives to conduct any such audit.

1.17 Term of Standing Offer

1.17.1 Period of the Standing Offer

The period of the Standing Offer is from award date until such time as Canada chooses to re-compete the Standing Offer, no longer deems the Standing Offer necessary, or proceeds with a different procurement vehicle.

Canada may, by notice in writing to all Standing Offer Holders cancel this Standing Offer by giving all Standing Offer Holders at least 30 calendar days’ notice of the cancellation

1.17.2 Changes to the Standing Offer (Evergreen Clause)

As a result of the Standing Offer being perpetual, from time to time, SSC may amend any part of the Standing Offer as a result of a policy notification, legislation, or procedural change. Any such change will not affect existing contracts in place prior to the date of change. Notification of such change will be sent to the Offer Holder via a generic email, and Canada will request the Offer Holder to endorse the proposed amendment.

Should an Offer Holder not agree with such modifications, and no longer wishes to be considered for requirements raised under the Standing Offer as a result of the changes, the Offer Holder will notify the Standing Offer Authority and this Offer Holder will no longer be on the list of Standing Offer Holders.

1.17.3 Delivery Points

Delivery will be made to delivery point(s) specified at Attachment A - Statement of Challenge, or in Call-ups issued against this Standing Offer.

1.18 Authorities

1.18.1 Standing Offer Authority

The Standing Offer Authority for the Standing Offer is **Michaela Criper**.

The Standing Offer Authority is responsible for the establishment of the Standing Offer, its administration and revisions, any changes to the Standing Offer must be authorized in writing by the Standing Offer Authority. The Standing Offer Authority is also the Contracting Authority for all Call-ups issued under this Standing Offer. Upon the making of a Call-up, as Contracting Authority, she/he is responsible for any contractual issues relating to individual Call-ups made against the Standing Offer by any Identified User. The Offeror must not perform Work in excess of or outside the scope of the Standing Offer based on verbal or written requests or instructions from anybody other than the Standing Offer Authority.

1.18.2 Project Authority

The Project Authority under any given call-up will be specified in that call-up.

The Project Authority is the representative of the department or agency (the Client) for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Project Authority; however, the Project Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a Contract amendment issued by the Contracting Authority.

1.18.3 Technical Authority

The Technical Authority for the Standing Offer is **Christopher Hardy**.

The Technical Authority is the representative of the Department of Justice who is responsible for all matters concerning the technical content under the Standing Offer. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the Standing Offer or to the scope of the Work under the Contract. Changes to the Standing Offer or

scope of Work can only be made through a Standing Offer or Contract amendment issued by the Contracting Authority.

1.18.3 Offeror's Representative

Victor Abou-Assaleh has been appointed as the representative for the Offeror and has full authority to act as agent for the Offeror regarding all matters relating to the Standing Offer.

1.19 Identified Users

The Identified Users authorized to make call-ups against the Standing Offer include any government department, agency or Crown Corporation listed in Schedules I, I.1, II, III, IV and V of the *Financial Administration Act*, R.S.C. 1985, c. F-11.

1.20 Price Adjustment Mechanism

At the request of the Offeror, the prices outlined in Attachment B - Basis of Payment, and the prices for Call-ups issued 24 months after the date of Standing Offer award, will be adjusted in accordance with the following Price Adjustment Mechanism.

The prices will be adjusted to account for inflation according to Table 18-10-0004-01 Consumer Price Index, monthly, not seasonally adjusted, All-items, Canada

$$\text{New Price} = \text{Initial Price} * \left(1 + \frac{\text{(CPI exercise date of the Option-CPI at the Standing Offer award)}}{\text{CPI at Standing Offer award}}\right)$$

For example:
The initial price for a Requirement - Work Segment 2 Call-ups is $ 1000.
Standing Offer award March 31, 2019.
A Work Segment 2 Call-up is issued on June 2, 2021.
CPI for March 2019 = 134 (hypothetical value)
CPI for May 2021 = 136
The new price = 1000 * (1+ (136-134) / 134) = $ 1,014.93

1.21 Exchange Rate Fluctuation

Canada assumes some of the risks and benefits of exchange rate fluctuation. The exchange rate fluctuation amount is determined in accordance with the provision of this article.

(a) From Standing Offer award to invoice payment(s), if raised by Canada or the Offeror, Canada will adjust the price(s); as specified in Attachment B - Basis of Payment, to reflect the exchange rate fluctuation, in Canadian dollars (CAD), if the exchange rate fluctuation is greater than 8% (increase or decrease) from the date of Standing Offer award. If either of the aforementioned dates fall on a Saturday, Sunday, or statutory holiday (non-Federal Government Working Days), Canada will calculate

the rate using the previous workday. The exchange rate adjustment amount will be calculated in accordance with the following formula:

adjustment = price(s) at standing offer award X (exchange rate for adjustment - initial exchange rate) / exchange rate for adjustment

(b) The initial exchange rate (CAD) is set as the daily average rate as published by the Bank of Canada on the Offer Closing date.

(c) Canada reserves the right to audit any price adjustments in accordance with the Accounts and audit provisions of the SACC 2030 (2020-05-28), General Conditions - Higher Complexity – Goods.

(d) This clause will only apply to the goods and services directly impacted by the exchange rate e.g., hardware, software, and certain operational maintenance and support services.

1.22 Evolving Basis of Payment

Canada will, at its sole discretion, validate the Solution's pricing components "components" outlined in Attachment B - Basis of Payment, during the Proof of Concept development, testing, and evaluation phase, and during the Standing Offer period. Where the validation exercise renders available variations, for example: any additions, updates, improvements on, bug patches, new versions of, or other modifications to the components, Canada reserves the right to modify those components, and as a result, the Offeror may propose price adjustments to those modified components.

1.23 Evolving Basis of Payment – Price Adjustment to Pricing Components

As per paragraph 1.23, the Offeror may propose price adjustments to the modified pricing components outlined in Attachment B - Basis of Payment. The Offeror's proposed price adjustments to the modified components, will be determined in accordance with the applicable principles for price justification, found in SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services - Competitive Requirements subsection 14 Price justification.

Adjustments to the modified components, may only be exercised by the Standing Offer Authority and will be evidenced, for administrative purposes only, through a Standing Offer amendment.

1.24 Direct Request by Customer Department

SACC A9117C (2007-11-30), T1204 - Direct Request by Customer Department

Is incorporated into the Standing Offer by reference.

1.25 Taxes - Foreign-based Contractor

SACC C2000C (2007-11-30), Taxes - Foreign-based Contractor

Is incorporated into the Standing Offer by reference.

1.26 Certifications of Compliance

Compliance with the Certifications provided by the Offeror is a condition of authorization of the Standing Offer and subject to verification by Canada during the entire period of the Standing Offer and of any resulting contract that would continue beyond the period of the Standing Offer. In the event that the Offeror does not comply with any certification or that it is determined that any certification made by the Offeror in its Offer is untrue, whether made knowingly or unknowingly, Canada will have the right to set-aside a Standing Offer and will have the right to terminate any resulting Contract for default.

1.27 COVID-19 Vaccination Requirement Certification Compliance

Canada will have the right to set-aside a Standing Offer, if the COVID-19 Vaccination Requirement Certification is or becomes untrue or if the Offeror fails to comply with such Certification during the period of any resulting Contract.

Canada will also have the right to terminate any resulting Contract for default if the COVID-19 Vaccination Requirement Certification is or becomes untrue or if the Contractor fails to comply with such Certification during the period of the Contract.

1.28 Applicable Laws

The Offeror must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

1.29 Foreign Nationals

SACC A2001C (2006-06-16) Foreign Nationals (Foreign Contractor)

Is incorporated into the Standing Offer by reference.

1.30 Insurance – No Specific Requirement

The Offeror is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the Standing Offer and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Offeror is at its own expense and for its own benefit and protection. It does not release the Offeror from or reduce its liability under the Standing Offer.

1.31 Safeguarding Electronic Media

(a) Before using them on Canada's equipment or sending them to Canada, the Offeror must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Offeror must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

(b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Standing Offer, including accidental erasure, the Offeror must immediately replace it at its own expense.

1.32 Priority of Documents

The Parties agree that only the conditions that expressly form part of the Standing Offer, by being written out in full in the Standing Offer or an Attachment or Annex to the Standing Offer, listed in the Priority of Documents section in the Standing Offer, form part of the Standing Offer.

If there is a discrepancy between the wording of any documents that appear on the list, the wording of the document that first appears on the list has priority over the wording of any document that subsequently appears on the list:

a) the Call-up against the Standing Offer, including any Attachments and Annexes;

b) the Standing Offer, including any Attachments and Annexes;

c) SACC 2005 (2017-06-21), General Conditions - Standing Offers - Goods or Services);

d) additional terms and conditions - approved by Canada, if applicable,

e) the Offeror's Offer dated November 10, 2021, not including any software publisher license terms and conditions that may be included in the Offer, not including any terms and conditions in the Offer with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the Offer.

SECTION 2 RESULTING CONTRACT CLAUSES

The following clauses and conditions apply to and form part of any Contract resulting from a Call-up issued against the Standing Offer.

2.1 Statement of Challenge

The Contractor must perform the Work described in the Call-up against the Standing Offer.

2.2 Standard Clauses and Conditions

2.2.1 General Conditions

The following General Condition is incorporated by reference.

SACC 2030 (2020-05-28), General Conditions - Higher Complexity - Goods

2.2.2 Supplemental General Conditions

The following Supplemental General Conditions are incorporated by reference.

SACC 4003 (2010-08-16), Supplemental General Conditions - Licensed Software

SACC 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software

SACC 4006 (2010-08-16), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information

SACC A9117C (2007-11-30), T1204 - Direct Request by Customer Department

SACC C2000C (2007-11-30), Taxes - Foreign-based Contractor

All references contained within the SACC 2030 (2020-05-28), General Conditions - Higher Complexity – Goods, or in any Supplemental General Condition, or in any Call-up Instrument (PWGSC-TPSGC 942 "Call-up Against a Standing Offer") or equivalent, to the Minister of Public Works and Government Services will be interpreted as a reference to the Minister of Digital Government presiding over SSC and all references to the department of Public Works and Government Services will be interpreted as a reference to SSC.

2.2.2.1 4003 Supplemental General Conditions - Licensed Software

(a) With respect to the terms and conditions of Supplemental General Conditions 4003 the following applies.

Licensed Software	The Licensed Software, which is defined in 4003, includes all the products offered by the Contractor in its Offer, and any other software required for those products to function in accordance with the Software Documentation and the Specifications, including without limitation all of the following products: 1. TitanFile Live
Type of License being Granted	User License, in accordance with section 04 of 4003.
Language of Licensed Software	The Licensed Software must be delivered in both English and French in accordance with the Statement of Challenge - Annex 4: Official Language Requirement.
Delivery Location	As specified in Attachment A - Statement of Challenge or AS per Individual Call-ups
Media on which Licensed Software must be Delivered	DVD, USB, or Internet link for download
Source Code Escrow	No

Required	

2.2.2.2 4004 Supplemental General Conditions - Maintenance and Support Services for Licensed Software

(a) The terms and conditions of Supplemental General Conditions 4004 are modified as follows.

Licensed Software	TitanFile Live
Hours for Providing Hot Line Support Services	In accordance with the Statement of Challenge - WS 2, section entitled Establishing the Help Desk (8AM to 5PM EST, Monday to Friday.)
Contact Information for Accessing the Contractor's Support Services	In accordance with section 05 *Support Services* of 4004, the Contractor will make its support services available through the following: Toll-free Telephone Access; Online Chat; and Email Access.
Website	In accordance with section 05 *Support Services* of 4004, the Contractor must make support services available over the Internet. To do so, the Contractor must include, as a minimum, frequently asked questions and on-line software diagnostic and support tools. Despite the Hours for Providing Hot Line Support Services, the Contractor's website must be available to Canada's users 24 hours a day, 365 days a year, and must be available 99% of the time. The Contractor's website address for web support is: www.titanfile.com
Language of Support Services	The Support Services must be provided in both French and English, based on the choice of the User requesting support.
Section 07, paragraph 1 of 4004: *Canada's Responsibilities*	Canada will not maintain, for the software support period, a telephone line and Internet access for use in connection with the software support services.

2.3 Term of Contract

2.3.1 Period of the Contract

The Work must be completed in accordance with the Call-Up issued against the Standing Offer.

2.3.2 Delivery Date

Delivery must be completed in accordance with the Call-up issued against the Standing Offer.

2.4 Payment

2.4.1 Basis of Payment

2.4.1.1 Basis of Payment - Limitation of Expenditure

- **WS 2 Call-ups - Deployment of the Operational Solution (User or Entity Based)**
  - **Secure File Transfer Solution - Annual Subscription Licenses (User or Entity Based)**
  - **Additional User Licenses**
- **Call-ups - Professional Services**
- **Call-ups - Virtual Training Services**

In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid the Firm All-Inclusive Price Per User or Firm All-Inclusive Price per Entity, as specified in Attachment B - Basis of Payment (as applicable). Canada's liability to the Contractor under the Call-ups against the Standing Offer must not exceed the limitation of expenditure specified in the authorized Call-up issued against the Standing Offer. Customs duties are included, and Applicable Taxes are extra.

No increase in the liability of Canada or in the price of the Work specified in the Call-up against the Standing Offer resulting from any design changes, modifications or interpretations of the Work will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been authorized, in writing, by the Standing Offer Authority before their incorporation into the Work.

2.4.1.2 Basis of Payment - Call-ups Solution Improvements

In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid; for improvements that are provided by the Contractor itself, the prices determined in accordance with the applicable principles for price justification, found in SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services - Competitive Requirements subsection 14 *Price justification*.

In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid; for improvements that are provided by a third-party (other than the Contractor), cost, plus a 5% mark-up.

2.4.1.3 Basis of Payment: Call-ups - Catch-All

In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid; for any non-listed items that are intended, in their entirety or in part, for the Secure File Transfer project, that are provided by the Contractor itself, the prices determined in accordance with the applicable principles for price justification, found in SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services - Competitive Requirements subsection 14 *Price justification*.

In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid; for any non-listed items that are or may be intended, in their entirety or in part, for the Secure File Transfer project, that are provided by a third-party (other than the Contractor), cost, plus a 5% mark-up.

2.4.2 Method of Payment

2.4.2.1 Advance Payment - Licensed Software (Solution)

Canada will pay the Contractor for the license(s) to use the Licensed Software (Solution), in accordance with Attachment B - Basis of Payment - WS 2 Call-ups - Deployment of the Operational Solution, payable in advance for each one year period if:

i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii) all such documents have been verified by Canada.

2.4.2.2 Single Payment – Professional Services

Canada will pay the Contractor upon completion and delivery of the Work, in accordance with Basis of Payment provisions for *Professional Services* if:

i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii) all such documents have been verified by Canada;

iii) the Work delivered has been accepted by Canada.

2.4.2.3 Single Payment - Virtual Training

Canada will pay the Contractor upon completion and delivery of the Work, in accordance with Attachment B - Basis of Payment - Virtual Training if:

i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii) all such documents have been verified by Canada;

iii) the Work delivered has been accepted by Canada.

2.4.2.4 Single Payment - Solution Improvements

Canada will pay the Contractor upon completion and delivery of the Work, in accordance with Basis of Payment provisions for *Solution Improvements* if:

i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii) all such documents have been verified by Canada;

iii) the Work delivered has been accepted by Canada.

2.4.2.5 Single Payment - Call-ups - Catch All

Canada will pay the Contractor upon completion and delivery of the Work, in accordance with Basis of Payment provisions for *Call-ups - Catch All* if:

i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

ii) all such documents have been verified by Canada;

iii) the Work delivered has been accepted by Canada.

2.5 Invoicing Instructions

The Contractor must submit invoices in accordance with the SACC 2030 (2020-05-28), General Conditions - Higher Complexity - Goods paragraph entitled *Invoice submission* instructions. The Contractor's invoice must include a separate line item for each element in the Basis of Payment provision of the Contract.

By submitting invoices (other than for any items subject to an advance payment), the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with

the Basis of Payment provision of the Contract, including any charges for Work performed by subcontractors.

Canada will only be required to make payment following receipt of an invoice that satisfies the requirements of this article.

The Contractor must submit invoices on its own form, which must include:

- the date;
- the Contractor name and address;
- the Destination
- Standing Offer number;
- financial codes, including GST or HST (as applicable) registration number;
- description of the Work
- category(ies) of personnel and number of days worked;
- Firm Per Hourly Rate on which the total dollar amount of the invoice is based;
- the amount invoiced (exclusive of the Goods and Services Tax (GST) or Harmonized Sales Tax (HST) as appropriate) and the amount of GST or HST, as appropriate, shown separately;
- Client Reference Number (CRN);
- Business Number (BN); and
- total value billed to date and the dollar amount remaining in the Contract to date.

The Contractor must send the original invoice to the Technical Authority's paying office as specified in the authorized Call-ups against the Standing Offer and one copy of the invoice to the Standing Offer Authority.

The original and copy of the invoice must be sent to the paying office as specified in the authorized Call-ups against the Standing Offer.

The Technical Authority's paying office as specified in the authorized Call-ups against the Standing Offer will send the invoices to the Technical Authority for approval and certification; the invoices will be returned to the paying office for all remaining certifications and payment action.

Any invoices where items or group of items cannot be easily identified will be sent back to the Contractor for clarification with no interest or late payment charges applicable to Canada.

If Canada disputes an invoice for any reason, Canada agrees to pay the Contractor the portion of the invoice that is not disputed provided that items not in dispute form separate line items of the invoice and are otherwise due and payable under the Contract. Notwithstanding the foregoing, the terms of the SACC 2030 (2020-05-28), General Conditions - Higher Complexity - Goods paragraph entitled *Interest on Overdue Accounts* will not apply to any such invoices until such time that the dispute is resolved at

which time the invoice will be deemed as “received” for the purpose of the *Method of Payment* clause of the Contract.

2.6 Limitation of Expenditure

Canada's total liability to the Contractor under the Contract must not exceed the total estimated expenditure as specified in each authorized Call-up issued against the Standing Offer, inclusive of any increase and decrease. Customs duties are included, and Applicable Taxes are extra.

No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications, or interpretations of the Work, will be authorized, or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Standing Offer Authority before their incorporation into the Work. The Contractor must not perform any Work or provide any service that would result in Canada's total liability being exceeded before obtaining the written approval of the Standing Offer Authority. The Contractor must notify the Standing Offer Authority in writing as to the adequacy of this sum:

when it is 75% committed, or
four months before the contract expiry date, or
as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,
whichever comes first.

If the notification is for inadequate contract funds, the Contractor must provide to the Standing Offer Authority a written estimate for the additional funds required. Provision of such information by the Contractor does not increase Canada's liability.

2.7 Limitation of Liability - Public Cloud Software as a Service (SaaS)

First Party Liability

Contract Performance: The Contractor is fully liable for all damages to Canada, arising from the Contractor's performance or failure to perform the Contract.

Data Breach: The Contractor is fully liable for all damages to Canada resulting from its breach of security or confidentiality obligations resulting in unauthorized access to or unauthorized disclosure of records or data or information owned by Canada or a third party.

Limitation Per Incident: Subject to the following section, irrespective of the basis or the nature of the claim, the Contractor's total liability per incident will not exceed the cumulative value of the Contract invoices for 12 months preceding the incident.

No Limitation: The above limitation of Contractor liability does not apply to:

- willful misconduct or deliberate acts of wrongdoing, and
- any breach of warranty obligations.

Third Party Liability

Regardless whether the third party claims against Canada, the Contractor or both, each Party agrees that it will accept full liability for damages that it causes to the third party in connection with the Contract. The apportionment of liability will be the amount set out by agreement of the Parties or determined by a court. The Parties agree to reimburse each other for any payment to a third party in respect of damages caused by the other, the other Party agrees to promptly reimburse for its share of the liability.

ATTACHMENT A
STATEMENT OF CHALLENGE
Secure File Transfer

---

1. Background

Canada has a requirement for a Secure File Transfer Solution ("Solution"). Large documents are being sent to and from Government departments and agencies and external stakeholders. The current process is very time consuming to ensure large files are being transferred in a secure manner and without any changes to the metadata. Canada is seeking a Solution that must provide secure, easy, and bi-directional transfer of large volumes of data. The metadata and forensic integrity must be preserved throughout the file transfer process.

2. Scope of the Contract

2.1 Scope

The scope of this Contract is to resolve the problem and address the challenges.

2.2 Problem Statement

Canada lacks the tools to securely, easily and bidirectionally transfer large volumes of data in various file types while preserving metadata and forensic integrity.

2.3 Challenge(s) specific to Solution

Annex 1 to this Statement of Challenge lists the minimum viable requirements (MVR) and what the Solution must do or must be able to do. Under the resulting Contract(s), the Contractor must satisfy all MVRs. In the sections below, Canada describes the expected outcomes that should be achieved and the challenges that should be addressed, however achieving those outcomes and challenges is not mandatory under the resulting Contract(s).

The capacity of a given Contractor to produce the expected outcomes will be one of the factors that will be considered in the framework to make the choice of the Solution to be deployed.

2.3.1 Expected Outcomes & Challenges to be Addressed

For a Bi-directional File Transfer System

Expectation 1: Securely transfer large volumes of files

Challenges to be Addressed:

- Inability to execute large volume file transfer
- Inability to execute individual file size transfers over 5MB
- Inability to send and receive large volume files easily from other networks
- Inability to send a multitude of file formats
- Lacking system compatibility
- Inability to work with various network transfer speeds
- Inability to execute the file transfer in a timely manner
- Loss of network connectivity resulting in an interruption of a file transfer, and how a resumption is achieved when connectivity is restored

Expectation 2: Track and trace a file transfer

Challenges to be Addressed:

- Inconsistent tracking of files from end-to-end of file transfer process
- Lack of confirmation of receipt of files

Expectation 3: A file transfer system that preserves meta-data and forensic integrity

Challenges to be Addressed:

- Ability to preserve meta-data
- Maintain file format integrity

Expectation 4: Easy to Use

Challenges to be Addressed:

- Inefficient processes
- Lacking an automated or easy process
- Lacking an ability to transfer based on classification of material (i.e., up to and including Protected B)

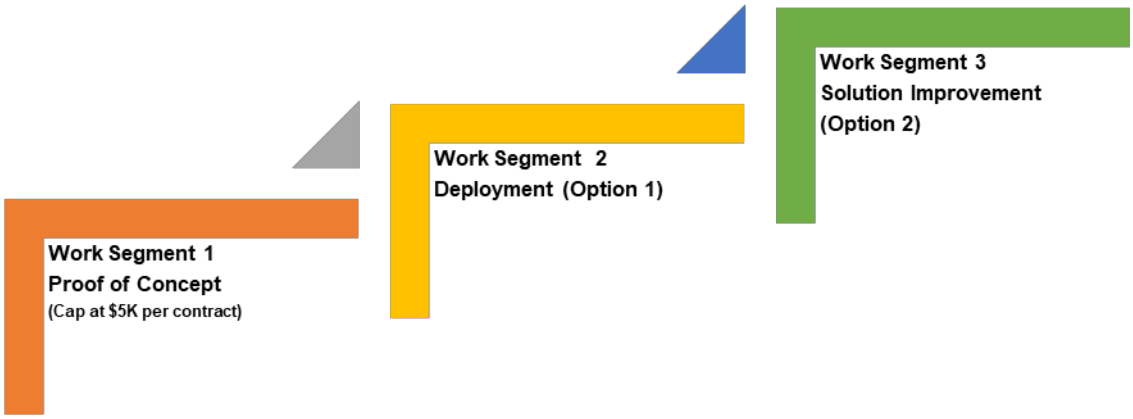
3. Process

Standing Offer Work Segments and Resulting Contracts

This Standing Offer (SO) is one of multiple SOs executed concurrently by various Offerors. At the end of the Proof of Concept (PoC) stage, Canada has determined what Solution(s) will be awarded a SO in accordance with the Decision-Making Framework (section 4.6). As described in the SO, the stages following the Proof of Concept will be actioned in accordance with Attachment A – Statement of Challenge.

The key Contract Work-Segments are the following:

[Note to Offerors: Work Segment 1 - Proof of Concept was completed on March 31, 2022, Section 4 Work Segment 1 – Proof of Concept in included for informational purposes only.]



4. Work Segment 1 – Proof of Concept

This section outlines the Contractor's obligation under the Solution Proof of Concept (Work Segment 1) and explains the mechanism used by Canada to determine which Solution is to be deployed under the Work Segments 2 – Deployment of the Operational Solution.

4.1 Location of Work & Duration

The Work for the Proof of Concept (PoC) will be conducted remotely. Acceptance testing of the PoC will be performed remotely by nationally distributed Users.

The duration of the PoC will not exceed 2 months.

4.2 Performance Assessment

The Contractor must demonstrate its Solution(s) satisfies MVRs – Annex 1.

Only a Solution that has satisfied all MVRs will be considered for future call-up allocation.

If no Solution can demonstrate that it satisfies all MVRs, Canada may choose to remove MVRs and apply the change to all Offerors.

4.3 Stages of Work Segment 1 - Solution Proof of Concept and Contractor's Roles and Responsibilities

The PoC is to be delivered in the 5 stages described below. Details of the PoC Deliverables are defined in section 4.5.

Stage 1 – Kick Off Meeting

The Contractor must:

- Participate in the virtual Kickoff meeting organized by Canada.
- Ask questions to ensure they have a clear understanding of deliverables.
- Discuss with Canada the Work as defined in this SoC and identify issues that need to be addressed.

Stage 2 – Planning the Testing

The Contractor must:

- Produce and provide the test plan and the user guide that will be needed by the test Users, as defined below in section 4.5
- Provide test scenarios and prerequisites
- Identify the functions of the Solution that will meet the PoC scenarios

Stage 3 - Installing/Preparing for the testing and assigning the licences

The Contractor must:

- Configure and set-up the Solution to be ready to deliver the PoC
- Provide licences for installation and use as requested by Canada that can manage a file transfer capacity of a minimum of 2TB
- Provide Canada with control of encryption keys
- Provide user guides and any additional training material as provided for in section deliverable below
- Deliver an orientation session to test Users at a date and time requested by Canada

Stage 4 – Testing and Documenting Results and Reporting

The Contractor must:

- Be available to provide the following support services
    - Experts available by email or phone from 9am to 5pm EST to answer questions that will provide guidance and assistance for troubleshooting issues/problems to the testing team throughout the testing stage.
    - Assist and resolve any gaps in the testing scenarios throughout the testing stage to satisfy scenario requirements.
- If Canada identifies MVRs that are not satisfied in the Testing Results Report, the Contractor must review the report and provide a Remediation Resolution Plan in response to Canada's Testing Results Report, within 10 calendar days from the date of receipt of the Testing Results Report to address and resolve deficiencies in meeting the MVRs and for retesting.

4.4 Canada's Roles and Responsibilities

In concurrence with the activities identified above, Canada will be responsible for the following:

Stage 1: Kickoff Meeting

- Organize the virtual Kickoff meeting
- Provide the test template
- Define the list of licenses that must be provided

Stage 2: Planning the Testing

- Define the types, volumes, and sizes of files for use during the PoC
- Define indicators of success for the Contractor provided scenarios
- Confirm Contractor provided test scenarios and provide any additional or modified scenarios required to validate the Use Cases.

Stage 3: Installing/Preparing for the testing and assigning the licences

- Provide the Contractor with the required number of licenses needed by Canada to conduct the PoC
- Assign the licenses to the PoC test Users
- As required for the Solution implementation, Canada will configure the encryption keys
- Distribute the user guides and training materials to the test Users
- Identify availability of and help coordinate the participants for the orientation session
- Mobilize the resources ready for testing
- Coordinate with the Contractor to validate the beginning of the testing

Stage 4: Testing, Documenting Results and Reporting

- Perform the testing
- Mobilize test Users (up to 10 at any given time) to execute testing using the User guide provided by the Contractor
- Document the results of the testing in a Testing Results Report and provide a copy to the Contractor for review
- Retest the MVRs as per the Contractor's Remediation Resolution Plan

4.5 Deliverables and Delivery Dates

The Contractor must produce the following deliverables.

	Deliverables	Delivery date
1	Test Plan	10 calendar days after contract award
2	User Guide	5 calendar days after contract award
3	Test scenarios and prerequisites	10 calendar days after contract award

4	Orientation session	15 calendar days after contract award
5	Licensing or access required for encryption keys and testing	15 calendar days after contract award
6	Remediation Resolution Plan in response to Canada's Testing Results Report	10 calendar days after receipt of Testing Results Report
7	Accessibility Roadmap	25 calendar days after contract award

The Contractor must produce the following deliverables:

1- Test Plan:

The Contractor must deliver a Test Plan that includes at least the following components:

- Use cases that will permit the PoC test Users (mobilized by Canada) to evaluate the requested functionality of the Solution.
- For each Use Case, a listing of functions that enable the functionality being tested, specifically identifying the steps a User would take to perform each Use Case.

2- User Guide

The Contractor must deliver a User Guide that includes at least the following components:

- Step-by-step instructions for the access and use of the Solution
- Instructions for licensed, administration and guest Users
- Troubleshooting

The Contractor may deliver any additional training material for test Users that they consider to be relevant. Should the Contractor wish to add training material, it must do so 10 calendar days after contract award.

3 - Test scenarios and prerequisites

The Contractor must deliver test scenarios and prerequisites in the Contractor's preferred format to successfully test and validate compliance of the Solution with the MVRs.

4- Orientation session:

The Contractor must deliver a virtual orientation session, during which it must present the following:

- Overview of the Solution
- Live demonstration
- Answer test Users' questions

5 - Licensing or access required for encryption keys and testing

The Contractor must deliver 10 licenses and access to the encryption key(s) to Canada in the Contractor's preferred format.

6 - Remediation Resolution Plan in response to Canada's Testing Results Report

The Contractor must deliver a Remediation Resolution Plan that provides a detailed response to how the Contractor will address the MVRs not met and identified in Canada's Testing Results Report.

7 - Accessibility Roadmap

The Contractor must deliver an accessibility roadmap that includes, at least, the following components:

1. Activities required to improve the Solution and comply with all accessibility requirements identified in Annex 3
2. Proposed schedule and milestones with their associated costs

Canada will provide a template for the Accessibility Roadmap.

4.6 Decision-Making Framework for Choosing Solution(s) to be Deployed in Work Segment 2

If Canada chooses to raise a call-up to proceed to Work Segment 2, Canada will use, among other things, the following decision-making framework for selecting which Standing Offer Holders' Solution(s) will be implemented.

Canada will be seeking to test the MVRs that each of the Standing Offer Holders committed to provide as part of their Solution. Only Solutions that satisfy the MVRs will be considered for deployment.

The choice of the Solution to be deployed will be made on the basis of "best fit" and may be considered against other options for deployment (i.e., options other than the proof of concepts developed under this series of Standing Offers). Canada will select the Contractor that has delivered a Solution that, in Canada's opinion, demonstrates best fit and the most benefits for the Government of Canada (GC). The Solutions will be compared against each other by Canada and the following factors will inform Canada's opinion regarding which Solution demonstrates best fit and the most benefits for the GC.

Decision Making Factors

Overall user experience: what is the overall user experience for the various personas and Solution administrators?

The following aspects will be considered:

- The perceived ease with which each persona/administrator can perform common tasks and actions;
- The time for each persona/administrator to achieve proficiency with the Solution; and
- Flexibility of the Solution to allow each persona/administrator to customize the user experience to their needs.

Deployment and Operation costs

The total cost includes the cost of the Solution, as well as other costs incurred by Canada to deploy, operate, and maintain the Solution. For example, other costs may include hardware, software, data transfer, data storage, training, professional services, and other related costs.

Demonstrated capacity of the proposed Solution to deliver the expected outcomes and address the identified challenges

Expectation 1: Securely transfer large volumes of data

Challenges to be Addressed:

- Inability to execute large volume file transfer
- Inability to execute individual file size transfers over 5MB
- Inability to send and receive large volume files easily from other networks
- Inability to send a multitude of file formats
- Lacking system compatibility
- Unable to work with various network transfer speeds
- Inability to execute the file transfer in a timely manner
- Loss of network connectivity resulting in an interruption of a file transfer, and how a resumption is possible when connectivity is restored

Expectation 2: Track and trace a file transfer

Challenges to be Addressed:

- Inconsistent tracking of files from end-to-end of process
- Lack of confirmation of receipt of files

Expectation 3: A file transfer system that preserves meta-data and forensic integrity

Challenges to be Addressed:

- Ability to preserve meta-data
- Maintain file format integrity

Expectation 4: Easy to Use

Challenges to be Addressed:

- Inefficient processes
- Lacking an automated or easy process
- Lacking an ability to transfer based on classification of material (i.e., up to and including Protected B)

Capacity (Time and Costs) required to deliver a Solution that complies with the accessibility requirements as demonstrated through the accessibility roadmap.
Capacity to satisfy cloud requirements
Any other factor that could contribute to a successful deployment or better addressing the problem and challenges.

5. Work Segment 2 – Deployment of the Operational Solution

This section outlines the Contractor's obligation under Solution Deployment (Work Segment 2)

5.1 Location of Work & Duration

The Work for the Deployment of the Operational Solution will be conducted remotely.

The configuration and deployment of the Solution contracted must be completed within 30 calendar days of Contract award. The duration of the operation will be specified in the call-up.

5.2 Performance Assessment

The Contractor must provide a fully operational Solution that satisfies the Minimum Viable Requirements indicated in Annex 1, include any additional functionality proposed by the Contractor in its technical bid, and integrated in this Contract by issuing a Call-up for WS 3 - Solution Improvements if applicable.

5.3 Stages of Work Segment 2 - Contractor's Roles and Responsibilities

A- Deployment

The Deployment is to be delivered in the 5 stages described below. Details of deliverables are defined in section 5.5.

Stage 1 - Departmental configurations

The Contractor must:

- configure the Solution to meet security and interface configurations provided by Canada, including two-factor authentication and encryption key hosting
- provide the cloud environment to host the Solution for approval by Canada

Stage 2 – Initial test of configuration

The Contractor must:

- Provide a system configuration procedure for Canada to implement the security and interface configuration

- Review the feedback report via email from Canada and provide a Plan to remediate deficiencies, if applicable
- Remediate the deficiencies reported by Canada from the execution of the system and interface configuration procedure, if applicable

Stage 3 – Receive and Distribute Licences

- The Contractor must:
    - deliver the required number of licenses to the admin User identified by Canada

Stage 4 –Training to Users

- The Contractor must:
    - Deliver the training materials for review, feedback, and approval by Canada, which includes, at a minimum:
        - a demonstration of the Solution and recorded video of the demonstration
        - a Quick Start Guide
        - an Administrator Guide
        - a User Guide
        - any additional training materials, as identified by the Contractor

Stage 5 - Establishing the Help Desk

The Contractor must provide technical support and troubleshooting of issues via email, online chat, or by phone through its helpdesk services during regular business hours, 8AM to 5PM EST, from Monday to Friday.

B- Operation

The Contractor must continue to provide the Solution for the duration of the Contract and provide the technical support and troubleshooting of issues via email, online chat, or by phone through its helpdesk services during regular business hours, 8AM to 5PM EST, from Monday to Friday.

5.4 Canada's Roles and Responsibilities

A- Deployment

In concurrence with the activities identified above, Canada will be responsible for the following:

Stage 1: Departmental Configurations

- Provide required security and interface configurations to the Contractor
- Approve the cloud environment where the Solution is hosted by the Contractor
- The Contractor **MUST HOST** its Solution on one of the following eight (8) approved Cloud Service Provider's environment (https://gc-cloud-services.canada.ca/s/gc-cloud-fa?language=en_US).
    - GC AWS (Amazon Web Services)
    - GC Microsoft
    - GC ThinkOn

- GC Oracle
- GC Salesforce
- GC IBM
- GC ServiceNow
- GC Google

Stage 2: Initial testing of configuration

- Execute the security and interface configuration procedure for the security and interface configuration provided by the Contractor
- Report via email on any deficiencies for remediation by the Contractor

After reviewing the Remediation report, identify to the Contractor any problematic issues.

Stage 3: Receive and Distribute Licenses

- Specify the number of required licenses
- Specify the User admin who will receive and allocate the licences purchased

Stage 4: Training to Users

- Coordinate participants for the Solution Demonstration
- Review, provide feedback, and approve the training materials
- Distribute the training materials

Stage 5: Establishing the Help Desk

Ensure the dissemination of Help Desk contact information, procedures, and hours of operation to Users.

B - Operation

Canada will receive and allocate the licences, up to the maximum licences purchased.

Canada will report to the Contractor's representative any issues identified during the Contract period to the Contractor.

5.5 Deliverables and Delivery Dates

The Contractor must produce the following deliverables.

	Deliverables	Delivery date
1	Licenses	5 calendar days after contract award
2	Solution Demonstration	10 calendar days after contract award
3	Training Materials	15 calendar days after contract award

4	Help desk contact information, procedures, and hours of operation	10 calendar days after contract award
5	Security and interface configuration	15 calendar days after contract award
6	Plan to address any deficiencies identified by Canada in the security and interface configuration	20 calendar days after contract award

1- Licenses

The Contractor must deliver the licenses purchased and provide authorization and access to use the Solution to an identified User admin who will receive and allocate the licenses to designated users.

2- Solution Demonstration

The Contractor must deliver a remote demonstration, in English, of its Solution to the User Admin and Users as identified by Canada. The Solution Demonstration must include at least the following components:

- Overview of the Solution
- Account creation and access
- End-to-end process to transfer and receive files between Users and with unlicensed recipients
- File removal and disposition settings
- Reporting and report customization
- Notification settings
- Administration settings and configurations
- Administrative logs and reporting functions
- Time for questions and answers

The Solution Demonstration must be provided in real-time to Canada and a recorded copy of the demonstration must be provided to Canada within 5 calendar days after the demonstration.

3 - Training Materials

The Contractor must deliver training materials for review, feedback, and approval by Canada, that include at least the following components:

- Quick Start Guide
  - For administrators
  - For users
- Administrator guide
  - Step-by-step instructions with screenshots for the administrator functions

    - Troubleshooting
- User guide
    - Step-by-step instructions with screenshots for the access and use of the Solution by all Users
    - Troubleshooting
- At the discretion of the Contractor, additional training materials that they consider to be relevant. Should the Contractor wish to add training material, it must do so within 10 calendar days after contract award.

The training materials delivered must satisfy the official languages requirements and the accessibility requirements (Annex 3 and 4, respectively) at time of delivery, unless the Accessibility Roadmap identifies a different delivery date acceptable to Canada for satisfaction of the accessibility requirement.

4 - Help Desk contact information, procedures and hours of operation

The Contractor must deliver help desk contact information, procedures and hours of operation in the Contractor's preferred format. The Help Desk deliverables must satisfy the official languages requirements and the accessibility requirements (Annex 3 and 4, respectively) at time of delivery, unless the Accessibility Roadmap identifies a different delivery date acceptable to Canada for satisfaction of the accessibility requirement.

5 – Security and Interface Configuration

The Contractor must provide a complete security and interface configuration procedure to be executed by Canada. This procedure must include any steps that Canada must take to configure the encryption keys and secure the Solution.

6 – Plan to address any deficiencies identified by Canada in security and interface configuration checklist

The Contractor must provide a plan on how it will address any deficiencies identified by Canada after executing the security and interface configurations checklist.

6. Work Segment 3 – Solution Improvement

Canada may raise a call-up Work Segment 3 for Solution Improvements including non-compulsory functionalities. If Canada chooses to raise a call-up against Work Segment 3, the following will apply.

6.1 Identification of Improvements

Canada encourages the Offeror to identify and propose improvements to the Solution by leveraging technological innovations that are not covered under the Standing Offer or resulting Contract(s) but could improve the problem and challenges resolution.

Where an Offeror could provide a solution improvement the Offeror may develop a Business Case. The Business Case developed by the Offeror must include at least the following components:

- description of the solution improvement;
- expected outcomes on the problem and challenges to be resolved;
- estimated costs;

- expected timelines and effort.

If the value for money and benefit to the problem and challenge resolution are demonstrated, Canada will amend the Standing Offer or resulting Contract(s) to provide those requirements in accordance with the terms and conditions of this Standing Offer including Attachment A - Statement of Challenge, and in accordance with Attachment B – Basis of Payment.

5. ANNEXES TO STATEMENT OF CHALLENGE

Annex 1: Mandatory Minimum Viable Requirements

DEFINITIONS

Able to: Expression that refers to a functionality, or a component, of the solution that must be available to be actioned by users.

End-to-end file transfer process: Refers to the actions of the solution to upload and transfer documents from a source location to a destination location.

Graphical User Interface (GUI): An interface through which a user interacts with electronic devices such as computers, hand-held devices, and other appliances. This interface uses icons, menus and other visual indicator (graphics) representations to display information and related user controls, unlike text-based interfaces, where data and commands are in text.

Metadata: Refers to the data that provides information about the file data, such as the file size, file format, file source, time, and date of creation.

Original File: refers to the file selected on the sender User's system for upload.

MINIMUM REQUIREMENTS FOR SECURE FILE TRANSFER SOLUTION

1. **Non-functional requirements**: The solution must:
    a. be a Software as a Service (SaaS)
    b. be web-based, not requiring the User to install any software
    c. be Commercially available off-the-shelf (COTS)
    d. allow non-licensed Guest Users to receive and send documents to licenced Users
    e. not allow document editing and collaboration within the Solution or if such functionality exists, must be disabled
2. **Capabilities**: The Solution must:
    a. perform bi-directional file transfer
    b. track file transfers
    c. record a chronological account of the end-to-end file transfer process
    d. provide reporting on the chain of custody during the end-to-end file transfer process that contains Users, Dates, Times, MD5 Hash. (i.e., who had access to the file, when)

e. store and archive files for a minimum of 6 months
f. store and archive audit logs for a minimum of 1 year

3. **Capabilities**: The Solution must be able to do the following:
    a. notify users of transfer errors, upload errors and completions, as they occur
    b. allow users to resume failed file transfers in the event of an interruption
    c. allow the User to specify the destination of a download

4. **Users**: The solution must support these distinct roles:
    a. User (user who can send and receive)
    b. Admin (user who may grant roles, see audit logs, also be User)
    c. Guest (unlicensed user or recipient, who may receive files and send files back to a User)
5. **Concurrent Users**: The solution must allow a minimum of 100 concurrent Users to send and receive files simultaneously, for each Call-up
6. **File Size**: The solution must:
    a. accept uploads of 50GB
    b. support an unlimited file transfer data size.
7. **Ease of Use:** The solution must:
    a. allow a new User to perform a transfer with less than one hour of training
    b. enable a Guest User to transfer or receive a file without training
    c. include a GUI to perform upload and transfer functions that does not require the User to make use of any command lines.
8. **Notifications**: the solution must be able to:
    a. notify Users
        i. when a transfer has been completed
        ii. when files have been downloaded
        iii. when errors are encountered
    b. send e-mail notifications to the User's provided e-mail address
9. **Preserve metadata:** The solution must preserve all original file metadata, end-to-end, throughout the transfer process.
10. **File Integrity:** The solution must preserve:
    a. the folder structure of the file(s) transferred
    b. the MD5 or SHA-1/256/512 signature, that must remain unchanged from end-to-end of the file transfer process

11. **Audit Logging**: The solution must record in an audit log:
    a. User's IP address in the transaction upload
    b. User's IP address in the transaction download
    c. Login ID/Authentication of Users involved in a file transfer
    d. Timestamp of transactions
    e. Errors and interruptions
    f. The completion status of the transfer
12. **Security**: The solution must:
    a. encrypt using AES 256, from end-to-end of the file transfer process
    b. provide two-factor authentication
    c. provide encryption keys hosted within Canada and either held or controllable by Canada
    d. store all data, in transit and at rest, within the Solution, and within Canada, including backup data

Annex 2: Personas

2.1 Persona Name: Alex

Lawyers from Other Federal Departments and Agencies

Demographics:

- Work on litigation with various departments and agencies.
- Share and receive large volumes of documents and be able to transfer files to courts and with internal and external clients.
- Looking for client facing external tool to be used nationally and internationally with unions, arbitration panels, provinces, courts
- Paralegal does most of the transfers

Goals	Challenges
• Establish project • Outside council are aware of new files uploaded • System for ease of uploading (drag and drop)	-Want certified as protected b, may be secret documents or cabinet confidence documents -Want facility security clearance -Document co-editing capability -Incorporate into 365 MS -Security -Control who had access to what files -Tracking functions (including who accesses what files) -Ensure system works with other parties' systems -Be able to send mass volumes of emails with certain

	number of attachments -Some departments that will transfer documents do not have sensitive info -Some information currently goes into and is managed by a tool within the federal government – this Solution is more for evidence management and for larger civil action, so some information does not go into it like judicial review & tribunal documents -Some documents are for non-litigation work – i.e., ATIP requests -Some legal clients are on separate networks (i.e., separate computers on another network) – no way to transfer from one network to another so still need a physical device to transfer -Transferring large volumes of docs from Justice to external council is difficult - Some departments may want a place to store information and have others access that information – a place to hold and organize files and allow access (a library for documents you are working on) while others already have a system for this already -Want instant access to documents when they are updated /changed -Version control - A way to integrate with current document management systems
Values • Ease of use • Simplicity (uploading and external users) i.e., be able to click on a link and share • Having responsive technical support (perhaps SLAs for response time)	**Fears** • Less user-friendly Solution • Degree of client capture and integration with MS is concerning • Security risks – adequate protection – not leaked out • Accidental send out (because it may be too easy to share info) • Timeliness – different users having to access the tool – easy to provide permissions to users while meeting security requirements

Expectations	Measures of Success
• Transfer large amounts of documents with ease • Have local control – file administrator can have control over how file transfer system is structured) - over how data is organization • Auto-resume (Especially if more than a gig at a time)	1. Ease of use (like a water heater where we do not think twice about it) 2. Timeliness (when need to meet court timelines) 3. Fewer inherent software limitations (i.e., number of characters, sub directories, etc.) • Not time consuming to figure out how to use – being able to get what we need to as complete as possible • Complete elimination of reliance on hardware • Lower transaction costs (fewer people and intermediaries involved) • Fewer steps in transferring

2.2 Persona Name: Marge
Paralegal and Legal Assistant

Demographics:

- Document review – large amounts of data and large sizes

Goals	Challenges
-Ease of use (sets of instructions so we are not calling IT all the time) -Helpdesk at our disposal immediately (sometimes late at night)	-Getting files and information to places safely without going through 10 people -Working from electronic documents with large volumes -Issue with people sending links to google drives and other shared cloud areas -Finding a process that will meet the security criteria for clients – things need to be sent through a portal or email with small email boxes

	-Roadblock during Covid – restriction that clients cannot physically go into Justice office now and are asking for digital copies only -Large boxes of docs in some files with numerous council inhouse – lot of exchange of material in play sometimes for decades (no one person consist in the file since inception) -Tracking every time, the file moves are extremely difficult and is currently tracked in excel spreadsheet -Opposing council wants to use digital docs -Restricted with what can be sent because of mailbox sizes – sending in bits and pieces is problematic (hard to track, piece back together and search) -In some cases, issues with large volumes of docs – can only send to litigation officer (and then they send to the auditor and need to make sure the auditor can receive it) and only certain people at Justice can use it -Sometimes sending it to generic inboxes (so do not know who will receive it) -Sometimes there are particular security receipts on files -Law firms want to send documents to Justice, and they assume we have a portal (but we do not – done on CDs) -Currently have password protected devices but then must call or email with password -Time differences make it challenging to track receiving of material – that actual human eyes received it (rather than just setting it aside) -Being able to communicate expectations to clients (along with meeting responsibilities to meet with respect to court) – expectation is that what they are providing is in the format Justice needs it in <u>Receipt:</u> -Clients and Justice want receipt that the message was received and read (esp. for certificates of service) -Receipt that can be printed off to put in the file or put into an email folder to show the transaction happened -Want to have acknowledgement that what they received is what they were expecting (that it looks right)

Values	**Fears**
- Would like it to be searchable and viewable (when you find document to be able to click and view it and be able to see connected documents) - Provide good service - Expectation of Justice to external entities – if we can give them easy to use and addresses their security concerns - A way to exchange of communication to facilitate exchange (rather than email and back to platform and then email)	-Knowing that it gets there in full form and getting a receipt of getting there in full form --Privacy concern and not having it be hackable -Wonder if I am doing it correctly -Making sure the passwords and authentication is being passed on properly (not our forte) – Am I going to be able to get in? -Hard to step away from paper – b/c we know the end user will see it the same way I see it (lack confidence that the end recipient receives the same view and look that I have)
Expectations - Be able to put in some sort of database and in electronic format - Authentication for logging in - Able to be used in every type of browser - Looks like something familiar (so it is easier to use and brings comfort to using a new tool)	**Measures of Success** 1) User friendly – young are tech savvy and others not 2) It can handle large volumes and lengths of docs 3) Docs land in the right person's hands and at the right security clearance (privacy & security) • Not getting additional emails or phone calls • Good for less technologically inclined clients • Does not require excessive walk through of the Solution • Want to have more confidence and trust in getting it to the right clients in a secure manner

2.3 Persona Name: Hal

IT Personnel within Justice

Demographics:

- Send and receive files to and from government (currently have some tools in place for departs and types of files)

Goals	Challenges
- To manipulate data (exchange evidence) – data and image structure to our own and upload to internal electronic storage Solution – need to adapt to clients' structure or Justice structure - Fully automated login process - Metadata cannot be altered or manipulated - Want something automated fully both ways (no manual login involved)	- One of the current Solutions is hard to automate and requires a virtual key. Provinces and organizations outside of govt does not like having to get a key - Not efficient - Not much virtual space so have to work off external drives which requires the use of more hops - Permission issues for transfer of files – does not have access to some shared drives - Server space is a limitation - Download file, work on it, and then transfer back – so lots of work and time (sometimes need to transfer files overnight) - If update is happening the transfer needs to be restarted - Lots of large audio and video file sizes - One of the current tools is down from time to time (Plus there is a cost involved because it is based on frequency and amount of data transferred) - Network transfer speeds are not the same across the country - Classified info is being mixed with non-classified – want ability to correctly transfer docs based on security classification and designation

Values	Fears
	- Virus threats - Currently no business continuity – need for redundancy and also so we do not have to resend if there is an outage
Expectations - Sanitization for viruses - Protected B, C and secret support - needs to support all levels of security - Do not need to over-protect information (not everything is classified) - Remediate spillage (be able scrub from system appropriately) - When there is a breach on a system we do not control, we need to be able to demonstrate to senior management that we took appropriate steps - Notification of downtime (so we know files are not being sent out or coming in) - Central location to access and exchange would be good – one point of entry	**Measures of Success** 1) Integrity of the system – data is intact (Did what was transferred over match with the sources?) 2) Length of time to transfer things (timeliness and speed) 3) Easy to support and onboard any users (low support overhead) - Seamless transfer of information - Ease of adoption - Cost is reasonable (can be covered by Justice or clients) - Auditing record that process is working - Proof sent to a third party (for court) - Work without crippling the other environments - Cannot freeze for big files - User-friendly interface – with typical interface (so employees do not need extra help to navigate the interface) - Fully automatable – when the file enters the system, system is notified, and the file can be moved – no manual intervention for system to work

2.4 Persona Name: Winston

Litigation Managers and eDiscovery coordinators (in external government departments)

Demographics:

- Loading documents into Justice Database, process documents, and coordinate with researchers on how to send to Justice
- Some don't have access to the Justice database, so metadata is put into Access (DB from record keeping system) or couriered to Justice or put-on shared drive
- Scanned documents, electronic native documents, paper documents, and DBs being transferred

Goals	**Challenges**
- Transfer docs from and to Justice	-Preserving metadata -Metadata gets modified easily -Using Justice DB is a long process– an external drive from Justice needs to be uploaded to Justice then sent back to external department -Some docs are on-site as well as off-site -Some docs are located across Canada - and need to go into area offices -Using unencrypted USB drives at times -Difficult to get everything on the first try -Secure file exchange involves working with IT and paralegals (and only 48 hours to access) – difficult to coordinate time -Encrypted USBs paralegals cannot unencrypt -Reaching out to IT increases timelines and complexity -Stressful process to send docs to Justice -Processes are manual (so need to rely on self to make sure everything is properly documented) -Compliance challenge: having different levels of security on drives is not in compliance
Values	**Fears** -Fear around timeliness – extremely difficult to meet timelines -Things getting lost -Not secure -Access issues – sometimes need special access and sometimes it expires – also need to determine who to get access from to get material to the right person -Not being able to live up to legal responsibilities to deliver to Justice -Lose everything on the USB keys

Expectations	Measures of Success
-Be able to do it remotely over VPN from anywhere (lots of remote working still) -Make sure it gets there -Easy to use – can just drop zip file and no size limitations (will not need to put docs into parts) -Zip file stays for a week before it goes away (so time for paralegal to pick up documents) -Automated workflow process – anything to feed back that says who picked it up and when it was picked up (metadata tracking) – currently tracking is manual in a spreadsheet -Short, easy-to-understand instructions -Easy to use (no need for IT) -Tool to validate that what we put in is exactly what is seen on our side as Justice -Nothing is missing, and nothing is corrupt	1. Easy to use (i.e., drag and drop) 2. Metadata is not changed (for eDiscovery) 3. Simple tool to transfer everything with no issues - Saves time and stress to send docs - Fully confident that everything was received - Ability to pull a report to show the facts and that it is successful - Legally we would be in compliance with information management practices (different levels of security on drives will be in compliance) – protected A, B and all levels of documents can be transferred in the Solutions - When we transfer something, we do not hear back from Justice – everything was copied, and it was good (do not hear from Justice and internal team)

2.5 Personas - Measures of Success

Marge	Alex
Paralegal and Legal Assistants 1. User friendly – young are tech savvy and others not 2. It can handle large volumes and lengths of docs 3. Docs land in the right person's hands and at the right security clearance (privacy & security) • Not getting additional emails or phone calls • Good for less technologically inclined clients • Does not require excessive walk through of the Solution • Want to have more confidence and trust in	*Lawyers from other Federal Departments* 1. Ease of use (like a water heater where we do not think twice about it) 2. Timeliness (when need to meet court timelines) 3. Fewer inherent software limitations (i.e., number of characters, sub directories, etc.) - Not time consuming to figure out how to use – being able to get what we need to as complete as possible - Complete elimination of reliance on hardware - Lower transaction costs (fewer people and intermediaries involved) - Fewer steps in transferring

getting it to the right clients in a secure manner	
Winston *Litigation Managers and eDiscovery coordinators* 1. Easy to use (i.e., drag and drop) 2. Metadata is not changed (for eDiscovery) 3. Simple tool to transfer everything with no issues - Saves time and stress to send docs - Fully confident that everything was received - Ability to pull a report to show the facts and that it is successful - Legally we would be in compliance with information management practices (different levels of security on drives will be in compliance) – protected A, B and all levels of documents can be transferred in the Solutions - When we transfer something, we do not hear back from Justice – everything was copied, and it was good (do not hear from Justice and internal team)	**Hal** *IT personnel* 1. Integrity of the system – data is intact (Did what was transferred over match with the sources?) 2. Length of time to transfer things (timeliness and speed) 3. Easy to support and onboard any users (low support overhead) - Seamless transfer of information - Ease of adoption - Cost is reasonable (can be covered by Justice or clients) - Auditing record that process is working - Proof sent to a third party (for court) - Work without crippling the other environments - Cannot freeze for big files - User-friendly interface – with typical interface (so employees do not need extra help to navigate the interface) Fully automatable – when the file enters the system, system is notified, and the file can be moved – no manual intervention for system to work

Annex 3: Accessibility Requirement

SSC has put in place a mechanism that will allow for progressive compliance to the *Accessibility Act*.

During the Proof of Concept Work Segment, the Contractor developed a roadmap, which will ensure their Solution becomes fully compliant with the Act. The capacity of the Contractor to fully comply in a timely manner with the Accessibility requirements will be one of the factors that will be considered for the selection of the Solution(s) to be deployed.

To be compliant with the provisions of the Accessibility Act, the Solution must meet, at a minimum, the following requirements.

a) All Information and Communication Technology (ICT) components of the Solution must conform with the relevant accessibility requirements of EN 301 549 (2018). These components include, but are not limited to, web-based dashboards, reports produced by the software, product documentation, and support services.
b) Information presented through visualizations, graphs, and dashboard widgets for example, must be made available through non-visual means. Providing an alternate output, which presents the information textually, is sufficient to meet this requirement. The text version must provide the same information as the visualized version.
c) Where documents are provided in more than one format, for example, a report provided in both PDF and Excel format, at least one of the formats must be accessible. The accessible version must provide the same information as the inaccessible version, and a notice must be posted indicating which format is accessible.

Annex 4: Official Languages Requirement

To be compliant, the Solution must meet, at a minimum, the following official languages requirements:

a) Users must be able to enter customizable text on dashboards and in reports in either English or French;
b) The Solution must include functionalities that allow Users to fully work in either English or French;
c) Users must be able to toggle between English and French from any given page;
d) Users must be able to set an official language of preference for the Solution's interface;
e) Users must be able to select an official language of preference when brought to the Solution prior to launching it;
f) the Solution must generate e-mails to Users in both official languages, as applicable;
g) Support Services (telephone, e-mail, chat, Web) must be available in either English or French; and
h) Training must be provided in both official languages, i.e., instruction and course material must be available in either English or French, or both, as specified by Canada.

In addition to the provisions of the Official Languages Act, the Solution must be able to process folder names and file names with French accents or diacritical marks.

Attachment A1 - Security Requirements

(Note to Offerors: as a result of the Standing Offer being perpetual, from time to time Canada may amend any Security Requirement provision outlined in any part of the Standing Offer as a result of a policy notification, legislation, procedural or technological change in accordance with the paragraphs entitled, Evolving Security Requirements (Evergreen), and Changes to the Standing Offer (Evergreen Clause).

The following Security Requirements must be met before Canada will exercise WS 2 Call-ups - Deployment of the Operational Solution (User or Entity Based).

1. The Contractor must, at all times during the performance of the Contract, hold a valid Designated Organization Screening (DOS) and obtain approved Document Safeguarding Capability at the level of PROTECTED B, issued by the Contract Security Program (CSP), Public Works and Government Services Canada (PWGSC).

2. The Contractor personnel requiring access to PROTECTED information, assets or sensitive site(s) must EACH hold a valid personnel security screening at the level of SECRET, or RELIABILITY STATUS, as required, granted or approved by the CSP, PWGSC.

3. The Contractor MUST NOT utilize its facilities to process, produce, or store PROTECTED information or assets until the CSP, PWGSC has issued written approval.

4. The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED B.

5. Data residency must be within Canada for the Protected B, Medium Integrity, Medium Availability (PBMM) Software as a Service (SaaS) solution.

6. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CSP/PWGSC.

7. The Contractor must comply with the provisions of the:

   (a) Attachment A1.1 - Security Requirements Check List, and Attachment A1.2 - Security Guide (if applicable);

   (b) Contract Security Manual (Latest Edition);

(c) CSP website: Security requirements for contracting with the Government of Canada, located at www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

NOTE: There are multiple levels of personnel security screenings associated with this file. In this instance, a security guide must be added to the SRCL clarifying these screenings. The security guide is normally generated by the organization's project authority and/or security authority.

NOTE: Any Contractor, or third party delivering Cloud-Based Solutions must be approved by Canada. Contractors must comply with the security requirements in the GC Security Control Profile for Cloud-Based GC IT Services for Protected B, Medium Integrity and Medium Availability (PBMM), for the scope of the proposed Commercially Available Software as a Service (SaaS) provided. Prior to contract award, the contractor must provide evidence, and confirmation to Canada of a Cloud Solution assessment using the Canadian Centre for Cyber Security (CCCS) - IT Assessment & Supply Chain Integrity (SCI) Assessment (ITSM.50.100) methodologies (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100) including the Treasury Board of Canada Secretariat defined security guardrails for cloud, performed by the Client Department, Shared Services Canada (SSC), or CCCS.

Furthermore, the Client Department IT Security Authority must perform a local IT assessment against the required controls, Guardrails, and cloud security profiles as determined by CCCS. Suppliers must provide the required information to the IT Security Authority upon request. For more information, guidance, and training on how to conduct this local IT assessment contact CCCS at contact@cyber.gc.ca.

Attachment A1.1 - Security Requirements Check List (SRCL)

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: 2BS-0-85236

Security Classification / Classification de sécurité

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Justice Canada	2. Branch or Directorate / Direction générale ou Direction: Information Solutions Branch (ISB)
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail
The purpose of this **CLOUD** procurement is to obtain a web-based COTS SaaS secure file exchange tool, permitting the bidirectional transfer of documents up to and including Protected B government departments and external third parties.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☑ No Non ☐ Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☑ No Non ☐ Yes Oui

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No Non ☑ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☑ No Non ☐ Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	☑ No Non ☐ Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☑	NATO / OTAN ☐	Foreign / Étranger ☐

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion ☑	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☑	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☑	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☐	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: 2BS-0-85236

Security Classification / Classification de sécurité

PART A *(continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B – PERSONNEL (SUPPLIER) / PARTIE B – PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☑ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET – SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments: / Commentaires spéciaux : CLOUD vendor will control the solution but content is encrypted. Secret clearance required for some cloud admins.

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — ☑ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?
If Yes, will unscreened personnel be escorted? — ☑ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

PART C – SAFEGUARDS (SUPPLIER) / PARTIE C – MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

11. b) Will the supplier be required to safeguard COMSEC information or assets? — ☑ No / Non ☐ Yes / Oui
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — ☑ No / Non ☐ Yes / Oui
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — ☐ No / Non ☑ Yes / Oui
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — ☑ No / Non ☐ Yes / Oui
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale?

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
2BS-0-85236
Security Classification / Classification de sécurité

PART C – *(continued)* / PARTIE C – *(suite)*

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category Catégorie	PROTECTED PROTÉGÉ			CLASSIFIED CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET	NATO RESTRICTED NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET COSMIC TRÈS SECRET	PROTECTED PROTÉGÉ A	 B	 C	CONFIDENTIAL CONFIDENTIEL	SECRET	TOP SECRET TRÈS SECRET
Information / Assets Renseignements / Biens		X														
Production																
IT Media / Support TI		X														
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No Non ☐ Yes Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No Non ☐ Yes Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
2BS-0-85236
Security Classification / Classification de sécurité

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Christopher Hardy	Director, Business Apps.	HARDY, Christopher Digitally signed by HARDY, Christopher Date: 2022.12.14 14:55:50 -05'00'

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
343-542-8558		christopher.hardy@justice.gc.ca	12/14/2022

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Sylvain Fournier	A/Director of SSEMD	Fournier, Sylvain

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-415-7626		sylvain.fournier@justice.gc.ca	

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☐ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
C. Jason Quade Contract Security Officer Jason.Quade@tpsgc-pwgsc.gc.ca		Quade, Clarence Digitally signed by Quade, Clarence Date: 2022.12.16 12:02:27 -05'00'

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Attachment A2 - Cloud Security Requirements

Cloud Security Requirements

(Note to Offerors: as a result of the Standing Offer being perpetual, from time to time Canada may amend any Security Requirement provision outlined in any part of the Standing Offer as a result of a policy notification, legislation, procedural or technological change in accordance with the paragraphs entitled, *Evolving Security Requirements (Evergreen),* and *Changes to the Standing Offer (Evergreen Clause).*

The Cloud Security Requirements outlined in the Standing Offer are applicable to the following Work Segments:

- WS 2: Deployment of the Operational Solution (User or Entity Based)

The following security requirements, if applicable, must be met in accordance with the Cloud Security Requirements, prior to Canada issuing WS 2 Call-ups.

Cloud Tiering Assurance Model

The Government of Canada (GC) Cloud Tiering Assurance Model (below) drives "cloud" security requirements, as well as the Canadian Centre for Cyber Security – Supply Chain Integrity, and the Public Service and Procurement Canada – Contract Security Program, activities.

For the purpose of this Solicitation, **Tier 2 - Protected B, Medium Integrity and Medium Availability** of the Cloud Tiering Assurance Model applies.

Requirements	Tier 2
GC Impact	Moderate
Categorization	Up to and including Protected B, Medium Integrity, Medium Availability
Data Residency	In Canada
Location	Off-premise
Deployment Model	Private, Public, Community, Hybrid
Service Model	SaaS
Compliance	ISO 27001 AND ISO 27017 AND SOC 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality
Privacy	ISO 27018

Certifications

The Offeror must demonstrate that the Solution complies with the requirements set forth in the following certifications and audit reports by providing independent third party assessment reports or certifications that addresses each service layer (e.g., IaaS, PaaS, SaaS) within the Cloud Service offering, including:

a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body; AND

b) ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services achieved by an accredited certification body; AND

c) AICPA Service Organization Control (SOC) 2 Type II Audit Report 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality - issued by an independent Certified Public Accountant.

d) Privacy – ISO/IEC 27018:2014 Information Technology - Security Techniques - Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors.

Cloud Service Provider (CSP) IT Security Assessment Program

a) The Offeror must demonstrate compliance with the security requirements selected in the Canadian Centre for Cyber Security (CCCS) Annex B Cloud Control Profile – Medium of the Guidance on Security Categorization of Cloud-Based Services (ITSP.50.103) (https://www.cyber.gc.ca/en/guidance/guidance-security-categorization-cloud-based-services-itsp50103) for the scope of the Cloud Services provided by the Offeror.

b) Compliance will be assessed and validated through the Canadian Centre for Cyber Security (CCCS) Cloud Service Provider (CSP) Information Technology (IT) Security Assessment Process (ITSM.50.100) (https://cyber.gc.ca/en/guidance/cloud-service-provider-information-technology-security-assessment-process-itsm50100).

c) The Offeror must demonstrate that they participated in the process by successfully on-boarded, participated in, and completed the program. This includes providing the following documentation:

(i) A copy of the confirmation letter that confirms that they have on-boarded into the program;
(ii) A copy of the most recent completed assessment report provided by CCCS; and
(iii) A copy of the most recent summary report provided by CCCS.

(Note to Offerors: For additional information on the Government of Canada security policy requirements in the context of cloud computing, please refer to the Treasury Board of Canada Secretariat – Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) - Canada.ca) and the Government of Canada Security Control Profile for Cloud-based GC Services - Canada.ca

Attachment B- Basis of Payment

1. Proof of Concept

For the Work described in the section entitled Work **Segment** 1 - Proof of Concept of the Statement of Challenge, Attachment A, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid the Firm All-Inclusive Lot Price, in Canadian funds, customs duty included, Goods and Services Tax, or Harmonized Sales Tax is extra, if applicable. The all-inclusive firm lot price includes the delivery of a Proof of Concept Solution. This delivery includes the usage rights, grants and access, training of users, the software documentation, warranty (if applicable), and maintenance and support, waivers, non-disclosure agreements and other releases to Canada for the purposes of conducting the Proof of Concept assessment. The price includes up to 10 User Licenses, as applicable, to use the Proof of Concept for assessment purposes during Work Segment 1 - Proof of Concept.

PROOF OF CONCEPT (PoC) FOR SECURE FILE TRANSFER (SFT) SOLUTION TABLE 1		
Proof of Concept	All deliverables associated with **Work Segment 1 - Proof of Concept**, in accordance with section entitled Work Segment 1 - Proof of Concept of the Statement of Challenge, Attachment A.	**Firm All-Inclusive Lot Price** **$ 5,000.00**

2A. Work Segment 2 – Deployment of the Operational Solution & Initial Contract Period (User License)

For the Work described in the section entitled Work Segment 2 – Deployment of the Operational Solution, of the Statement of Challenge, Attachment A, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a Firm All-Inclusive Price Per User, in Canadian funds, customs duty included, Goods and Services Tax, or Harmonized Sales Tax is extra, if applicable. The all-inclusive firm price per user includes; whenever applicable to the proposed Solution delivery model, all User Licenses, delivery, installation, integration and configuration of the Solution, incidental and additionally required information technology infrastructure services, software documentation, warranty, maintenance and support, training during Solution implementation period, waivers, non-disclosure agreements, and other releases to Canada, to access and use the Solution in accordance with the Contract.

DEPLOYMENT OF SOLUTION & INITIAL CONTRACT PERIOD (1 YEAR) TABLE 2A			
Work Segment 2 – Deployment of Solution	**Firm All-Inclusive Price Per User for the delivery of the Full SFT Solution**	**Total Number of Users – Initial Contract Period (1 Year)**	**Price per User**
1	Delivery of the Full Secure File Transfer Solution – 1 Year	**1 - 500**	$270.00
2	Delivery of the Full Secure File Transfer Solution – 1 Year	**501 - 1000**	$229.50
3	Delivery of the Full Secure File Transfer Solution – 1 Year	**1001 - 2000**	$189.00
4	Delivery of the Full Secure File Transfer Solution – 1 Year	**2001 - 5000**	$148.50

Note: For the Deployment of the Solution and Initial Contract Period, Table 2A will be used to determine the per user pricing. Ranges of Total Number of Users have been provided to capture pricing models that may offer varying prices depending on the User base size. For example, if a Deployment of 1500 Users is required, the Price per User of Table 2A, item 3 (1001-2000 Users) shall be used to determine the Price per User for all 1500 Users.

2B. Work Segment 2 – Deployment of the Operational Solution & Initial Contract Period (Entity License)

For the Work described in the section entitled Work Segment 2 – Deployment of the Operational Solution, of the Statement of Challenge, Attachment A, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a Firm All-Inclusive Price per Entity, in Canadian funds, customs duty included, Goods and Services Tax, or Harmonized Sales Tax is extra, if applicable. The all-inclusive firm price per entity includes; whenever applicable to the proposed Solution delivery model, an entity license, delivery, installation, integration and configuration of the Solution, incidental and additionally required information technology infrastructure services, software documentation, warranty, maintenance and support, training during Solution implementation period, waivers, non-disclosure agreements, and other releases to Canada, to access and use the Solution in accordance with the Contract.

DEPLOYMENT OF SOLUTION & INITIAL CONTRACT PERIOD (1 YEAR) TABLE 2B			
Work Segment 2 – Deployment of Solution	**Firm All-Inclusive Price Per Entity for the delivery of the Full SFT Solution**	**Entity Base Size Initial Contract Period (1 Year)**	**Price per Entity**
1	Delivery of the Full Secure File Transfer Solution – 1 Year	**Small Entity Max. 500 Devices/Users**	n/a
2	Delivery of the Full Secure File Transfer Solution – 1 Year	**Medium Entity Max. 3000 Devices/Users**	n/a
3	Delivery of the Full Secure File Transfer Solution – 1 Year	**Large Entity 3001 + Devices/Users**	n/a

Note: For the Deployment of the Solution and Initial Contract Period, Table 2B will be used to determine the per entity pricing. Entity Base Sizes (small, medium and large) have been provided to capture pricing models that may offer varying prices depending on the Entity Base Size. For example, if a Deployment of Medium Entity is required, the Entity License Price of Table 2B, item 2 (Medium Entity) shall be used.

For the purposes of determining the appropriate Entity Base Size, the Treasury Board of Canada Secretariat - Federal Public Service: Annual Population by Department statistics shall be used. (Population of the federal public service by department - Canada.ca)

Unless provided otherwise in the Contract, an "Entity License" entitles the Client to use the Licensed Software for government purposes throughout the entity in association with any number of Devices or by any number of Users. The Entity License allows the Client to use the Licensed Software in whole or in part, unrestricted by the number or type of Users, data, documents and/or transactions a Client or a User may be using or processing at any time, or the location of the Device.

3A. Secure File Transfer (SFT) - Annual Subscription User Licenses – Beyond Initial Year (Use License)

For the Contractor to deliver the Secure File Transfer - Annual Subscription User Licenses, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the

Contractor will be paid a Firm All-Inclusive Price Per User, in Canadian funds, customs duty included, Goods and Services Tax, or Harmonized Sales Tax is extra, if applicable.

SFT - ANNUAL SUBSCRIPTION USER LICENSES – BEYOND INITIAL YEAR Table 3A			
Annual Subscription User Licenses	**Firm All-Inclusive Price Per User for the delivery of Annual Subscription User Licenses**	**Total Number of Users – Beyond Initial Year**	**Price per User**
1	Annual Subscription Licenses as per Attachment A - Statement of Challenge	**1 - 500**	$270.00
2	Annual Subscription Licenses as per Attachment A - Statement of Challenge	**501 - 1000**	$229.50
3	Annual Subscription Licenses as per Attachment A - Statement of Challenge	**1001 - 2000**	$189.00
4	Annual Subscription Licenses as per Attachment A - Statement of Challenge	**2001 - 5000**	$148.50

Note: For any period beyond the Initial Contract Period, Table 3A will be used to determine the per user pricing. Ranges of Total Number of Users have been provided to capture pricing models that may offer varying prices depending on the User base size. For example, if after a Deployment and Initial period of 1500 users, an increased total amount of 3,000 users is required for another period, the Price per User of Table 3A, item 4 (2001-5000 Users) shall be used.

3B. Secure File Transfer (SFT) - Annual Subscription Entity License – Beyond Initial Year (Entity License)

For the Contractor to deliver the Secure File Transfer - Annual Subscription Entity License, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a Firm All-Inclusive Price per Entity, in Canadian funds, customs duty included, Goods and Services Tax, or Harmonized Sales Tax is extra, if applicable.

SFT - ANNUAL SUBSCRIPTION ENTITY LICENSE – BEYOND INITIAL YEAR TABLE 3B			
Annual Subscription Entity License	**Firm All-Inclusive Price Per Entity for the delivery of Annual Subscription Entity License**	**Entity Base Size Beyond Initial Year**	**Price per Entity**
1	Annual Subscription Entity License as per Attachment A - Statement of Challenge	**Small Entity** **Max. 500 Devices/Users**	n/a
2	Annual Subscription Entity License as per Attachment A - Statement of Challenge	**Medium Entity** **Max. 3000 Devices/Users**	n/a
3	Annual Subscription Entity License as per Attachment A - Statement of Challenge	**Large Entity** **3001 + Devices/Users**	n/a

Note: For any period beyond the Initial Contract Period, Table 3B will be used to determine the per entity pricing. Entity Base Sizes (small, medium and large) have been provided to capture pricing models that may offer varying prices depending on the Entity Base Size. For example, if a Deployment of Medium Entity is required, the Entity License Price of Table 3B, item 2 (Medium Entity) shall be used.

For the purposes of determining the appropriate Entity Base Size, the Treasury Board of Canada Secretariat - Federal Public Service: Annual population by Department statistics shall be used. (Population of the federal public service by department - Canada.ca)

Unless provided otherwise in the Contract, an "Entity License" entitles the Client to use the Licensed Software for government purposes throughout the entity in association with any number of Devices or by any number of Users. The Entity License allows the Client to use the Licensed Software in whole or in part, unrestricted by the number or type of Users, data, documents and/or transactions a Client or a User may be using or processing at any time, or the location of the Device.

4. Grant for Additional User Licenses

For the Contractor to deliver Additional User Licenses, and in consideration of the Contractor satisfactorily completing its obligations under the Contract, the Contractor will be paid a Firm All-Inclusive Pro-Rated Price Per User, in Canadian funds, customs duty included, Goods and Services Tax, or Harmonized Sales Tax is extra if applicable.

ADDITIONAL USER LICENSES TABLE 4			
Additional User Licenses	**Firm All-Inclusive Pro-Rated Price Per User for the delivery of Additional User Licenses**	**Total Number of User Licenses**	**Price per User (Pro-Rated if procured mid-period.)**
1	Additional User Licenses as per Attachment A - Statement of Challenge	**1 - 500**	$270.00
2	Additional User Licenses as per Attachment A - Statement of Challenge	**501 - 1000**	$229.50
3	Additional User Licenses as per Attachment A - Statement of Challenge	**1001 - 2000**	$189.00
4	Additional User Licenses as per Attachment A - Statement of Challenge	**2001 - 5000**	$148.50

Note: For both the Deployment and Initial Contract Period, as well as during any periods beyond the Initial Contract Period, if additional users are required, the Table 4 will be used to determine the per user pricing of those additional Users. Ranges of Total Number of Users have been provided to capture pricing models that may offer varying prices depending on the user base size. For example, if 1900 User Licenses are purchased for the Deployment and Contract Period, and 500 additional User Licenses are required mid-year (2400 total), the Price per user of Table 4, item 4 (2001-5000 Users) shall be used to determine the Price per Additional User.

5. Professional Services

For professional services requested by Canada, in accordance with a validly raised Call-up Instrument and the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor the firm price (travel and living expenses excluded), as set out in the Call-up Instrument, based on the Firm All-Inclusive Per Diem Rates in Canadian funds, Goods and Services Tax, or Harmonized Sales Tax is extra. Partial days will be prorated to actual hours worked based on a 7.5-hour workday.

PROFESSIONAL SERVICES (PS) TABLE 5	
Firm All-Inclusive Price in CAD (applicable taxes extra) per diem rates for PS to be provided on an as-and-when requested basis, in accordance with the terms and conditions of any **Professional Service Call-up(s)**, and including the section entitled *Professional Services*, of the Statement of Challenge, Attachment A.	
PS Category Description	**Per Diem Firm All-Inclusive Price**
IT Consultant (20)	$1,125.00
Application Architect (20)	$1,125.00
Data Specialist (20)	$1,125.00

Note: For evaluation purposes: during the initial contract period (1 year) and one annual subscription period, 20 represents the estimated Level of Effort in days for each category.

6. Optional Virtual Training Services

For training services requested by Canada, in accordance with a validly raised Call-up Instrument and the Contractor satisfactorily completing its obligations under the Contract, Canada will pay the Contractor the firm price (travel and living expenses excluded), as set out in the Call-up Instrument, based on the Firm All-Inclusive Price Per Trainee in Canadian funds, Goods and Services Tax, or Harmonized Sales Tax is extra.

OPTIONAL VIRTUAL TRAINING SERVICES TABLE 6	
Firm All-Inclusive Price in CAD (applicable taxes extra) per User for **Virtual Training Services** to be provided on an as-and-when requested basis, in accordance with the terms and conditions of any Virtual Training Service Call-up(s), and including the section entitled *Virtual Training Services*, of the Statement of Challenge, Attachment A.	
Training Category Description	**Firm All-Inclusive Price per Trainee**
Self-Led Training for Users (100)	$0.00
Self-Led Training for Administrators (100)	$0.00
Trainer-Led Training for Users (10)	$5.00
Trainer-Led Training for Administrators (10)	$0.00

Note: For evaluation purposes: during the initial contract period (1 year) and one annual subscription period, 100 represents the estimated number of trainees for Self-Led Training for Users, and Trainer-Led Training for Users, and 10 represents the estimated number of trainees for Self-Led Training for Administrators, and Trainer-Led Training for Administrators.

7. Limitation of Price

Canada will not pay the Contractor for any design changes, modifications, or interpretations of the Work unless they have been approved, in writing, by the Standing Offer Authority before their incorporation into the Work.

Attachment C - SCSI Vendor Submission Form

The following SCSI was submitted:

a) an IT Product List.

Attachment C - Supply Chain Security Information (IT Product List) - Incorporated by Reference.