Shared Services Canada

Challenge-Based Solicitation (CBS) – Prequalification
IaaS – Native PaaS

Solicitation No.	CS-IAAS-2024	Date	April 19, 2024
Issuing Office	Shared Services Canada 400 Cooper St, 6th Floor Ottawa, Ontario K2P 2H8		
Contracting Authority (The Contracting Authority is the person designated by that title in the Solicitation, or by notice to the Bidders, to act as Canada's "Contact" for all aspects of the Solicitation process.)	Cloud Services Team Manager: Nadia Kelly Team Lead: Khady Sy		
	Email Address: PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca		
Prequalification Closing Date and Time	May 13, 2024, 2:00 p.m. EDT		

Table of Contents

INTRODUCTION

Note to the Reader

Following the posting of an Initial Challenge-Based Solicitation (CBS) on CanadaBuys, Canada has received feedback from vendors and factored it in the update of the CBS.

This CBS aims to prequalify Bidders.

Only the prequalification process is detailed in this document.

Executive summary

As described under 1.4 – Challenge Based Solicitation Stages, Stage 4 is the fourth stage of this Challenge-Based Solicitation process, inviting Bidders interested in this requirement to qualify. The objective of this Prequalification stage is to establish a qualified pool of Bidders who have demonstrated their capacity to resolve the problem statement(s) and are deemed the most qualified in accordance with the requirements of this solicitation.

Once the prequalified Bidders are identified, Canada will work with them to develop the selection process that will result in the award of 2 or 3 Task Authorization Contracts.

Information Webinar

Bidders are invited to attend an Information Webinar to discuss the Prequalification Challenge-Based Solicitation. The Bidders must register by contacting the Contracting Authority prior to the date of the Webinar.

The Information Webinar will be held on the following dates and times:

a) The French-language webinar will be held on April 24, 2024, at 10:00 a.m. DST

b) The English-language webinar will be held on April 24, at 1:00 p.m. DST

Conflict of Interest and Unfair Advantage

As set out in the Standard Instructions 2003, a bid can be rejected due to an actual or apparent conflict of interest or unfair advantage.

In this regard, Canada advises that it has used the services of a number of private sector consultants/contractors in preparing strategies and documentation related to this procurement process, including the following:

- Adirondack (Sub-Contractor: CloudWise Consulting Ltd.)
- Agilipro (9421-5340 Québec Inc.)
- Lightning Tree (Sub-Contractors: Spring2Innovation to Gestion UniVision Management Inc.)
- Maplestream Inc., Cofomo Inc. IN JOINT VENTURE (Sub-Contractor: Partners in Procurement)
- TekSystems (Sub-Contractor: Robert Hilborn Consulting Inc.)
- The Lansdowne Consulting Group Inc.

SECTION 1 – GENERAL INFORMATION

1.1 Requirement

This bid solicitation is to establish contract(s) with task authorizations (TA) for the delivery of Infrastructure as a Service (IaaS) and Native Platform as a Service (PaaS) services to the Government of Canada.

Refer to Annex B – Statement of Challenge (SoC) for a detailed description of the requirement.

1.2 Structure of the Challenge-Based Solicitation

The Solicitation is divided into six Sections plus attachments and annexes.

Section 1: General Information; provides a general description of the requirements.

Section 2: Instructions to Bidders; provides the instructions, clauses, and conditions applicable to the Solicitation.

Section 3: Bid Preparation Instructions; provides Bidders with instructions on how to prepare their Bid.

Section 4: Evaluation Procedures and Basis of Selection; describes how the evaluation will be conducted, the evaluation criteria that will be used, and the basis of selection for Contract award.

Section 5: Certifications and Additional Information; includes the certifications and additional information to be provided.

Section 6: Resulting Contract Clauses; includes the clauses and conditions that will apply to any resulting Contract.

1.3 Solicitation Process

Unlike a traditional procurement, a Challenge-Based Solicitation (CBS) is based on the concept that Canada can best develop procurement artifacts, if it presents the requirement as a need (problem statement(s)) and allows industry the freedom to propose innovative solutions that fill the need. CBSs are accompanied with details outlining such activities and expectations, including but not limited to, industry participation or engagement, and evaluation methodologies. Solutions typically take the form of “Proof of concept” or demonstrations, and evaluations assess how well these satisfy the need.

Throughout the Invitation to Refine (ItR), Bidders are invited to provide feedback by participating in videoconference interactions, answering surveys, and other types of activities facilitated by Canada, in order to help Canada finalize the Challenge-Based Solicitation. Acceptance of Attachment 2 – Rules of Engagement will be requested for participating in the ItR.

Following multiple waves of ItR, the Final Challenge-Based Solicitation will be issued which includes details on the evaluation methodology that will be used to select resulting Contractors.

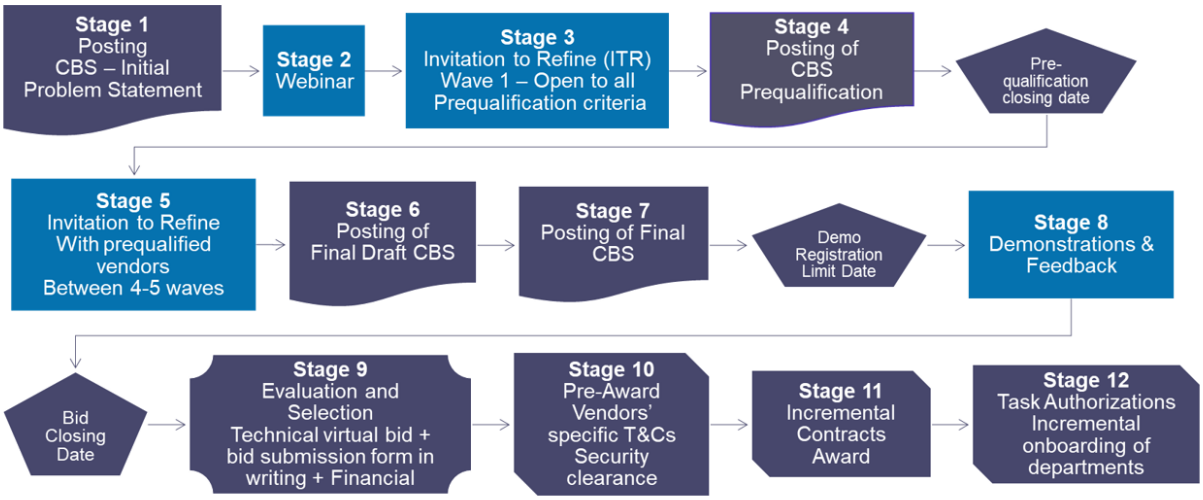
Evolving solicitation document

The solicitation document will evolve during the solicitation period. Below shows the various forms it will take:

1. Challenge-Based Solicitation (CBS) – Initial
2. CBS for Prequalification (CURRENT DOCUMENT)
3. Draft Final CBS
4. Final CBS

1.4 Challenge-Based Solicitation Stages

Table 1 - IaaS & Native PaaS Challenge Based Solicitation (CBS) Process



Stage 1: Challenge-Based Solicitation – Initial (Completed)

The Notice of Proposed Procurement (NPP) and Challenge-Based Solicitation (CBS) – Initial was published on www.canadabuys.canada.ca.

Stage 2: Information Webinar (Completed)

Bidders were invited to attend an Information Webinar during which Canada provided an overview of the approach, explained the Invitation to Refine (ItR) “waves,” and gathered feedback from industry on the proposed Solicitation process and evaluation framework.

Stage 3: Invitation to Refine – Wave 1 (Completed)

During Wave 1, Bidders were invited to provide feedback on the problem statement(s) and prequalification criteria and share their perspectives by participating in various interactive events (videoconferences, group interactions, surveys and Bidder presentations)

facilitated by Canada, in the presence of all Bidders. Bidders' feedback and presentations were not scored nor considered in the Solicitation evaluation process; ItR questions and answers were documented and provided to all Bidders. The purpose of the ItR (Wave 1) was to help Canada finalize the Prequalification CBS.

Stage 4 : Posting of CBS Prequalification (CURRENT STAGE)

Based upon the findings from ItR – Wave 1, Canada is now inviting Bidders to qualify. The objective of the Prequalification stage is to establish a qualified pool of Bidders who have demonstrated their capacity to resolve the problem statement(s) and are deemed the most qualified in accordance with the requirements of this solicitation.

Refer to Section 3 – Bid Preparation Instructions, for information on the submission process.

Canada will select the five most qualified Bidders for pool formation, in accordance with Section 4.1, Evaluation Procedures - Prequalification. Canada will notify Bidders not selected to form the pool, of their exclusion from further participation in the Challenge-Based Solicitation process.

From that point of the process, all communication related to the solicitation will occur between Canada and the prequalified Bidders. There will be no further postings on CanadaBuys until contract award.

Stage 5: Invitation to Refine (ItR) – Waves 2 and subsequent waves with prequalified Bidders

During the period of Waves 2 +, prequalified Bidders will be invited to provide additional feedback on the problem statement(s) and share their perspectives by participating in additional interactive events facilitated by Canada (in the presence of all prequalified Bidders or "one-on-one"). Bidders' feedback and presentations will not be scored nor considered in the Solicitation evaluation process; ItR questions and answers will be documented and provided to all Bidders. The purpose of the ItR (Waves 2 and subsequent waves) is to help Canada finalize the Challenge-Based Solicitation. The order and content of waves may be changed as required, and one or more waves may be concurrent.

Invitation to Refine – Description of Waves

Wave 1	Prequalification criteria; problem statement challenges and initial Minimum Viable Requirements (Completed)
Wave 2	Security and Privacy
Wave 3	Statement of Challenge
Wave 4	Terms and Conditions, Greening, Accessibility, Official Languages
Wave 5	Work Allocation Process
Wave 6	Price Monitoring and Financial Evaluation
Wave 7	Bid Evaluation Framework

Wave 8 Socio-economic Considerations

Wave 9 Supporting small departments and other levels of government (OLG)

As the development of the solicitation evolves, some ItR waves may be added, or removed as required.

Stage 6: Posting of DRAFT Final Challenge-Based Solicitation

At Stage 6, based on observations during the ItR events, Canada will refine and issue the Draft Final Challenge-Based Solicitation. Prequalified Bidders will have one last chance to share their feedback on the solicitation.

Wave 10 Draft Final CBS

Stage 7: Posting of Final Challenge-Based Solicitation

At Stage 7, based on feedback from stage 6, Canada will refine and issue the Final Challenge-Based Solicitation to the Prequalified Bidders.

Stage 8: Demonstration and Feedback

During stage 8, Canada will invite registered Prequalified Bidders to make their demonstration.

Prequalified Bidders will have up to the Demo registration date to register for the demonstration. The demonstration is mandatory in order to bid.

Demonstrations will be managed in accordance with the instructions of Section 4 - Evaluation Procedures and Basis of Selection.

Stage 9: Evaluation and selection

During stage 9 Canada will assess the Bids.

The highest ranked Prequalified Bidders, following the process detailed in Section 4, Evaluation Procedures and Basis of Selection, will be notified (*Notification of Selection*) of Canada's intent to award multiple Contracts.

Stage 10: Pre-award

During the Pre-award stage, Bidders notified of selection at Stage 9 will:

- submit their written Technical Bid that will be attached to the contract (Note to Bidders: Bidder's written Technical Bids are not to be provided at Bid Closing)
- If applicable, finalize the negotiation of Bidders' specific Terms and Conditions to be included in the resulting contract as the last element of the Priority of Documents.
- Validate the required security clearance.
- Validate compliance with certifications

Stage 11: Incremental Contract Award

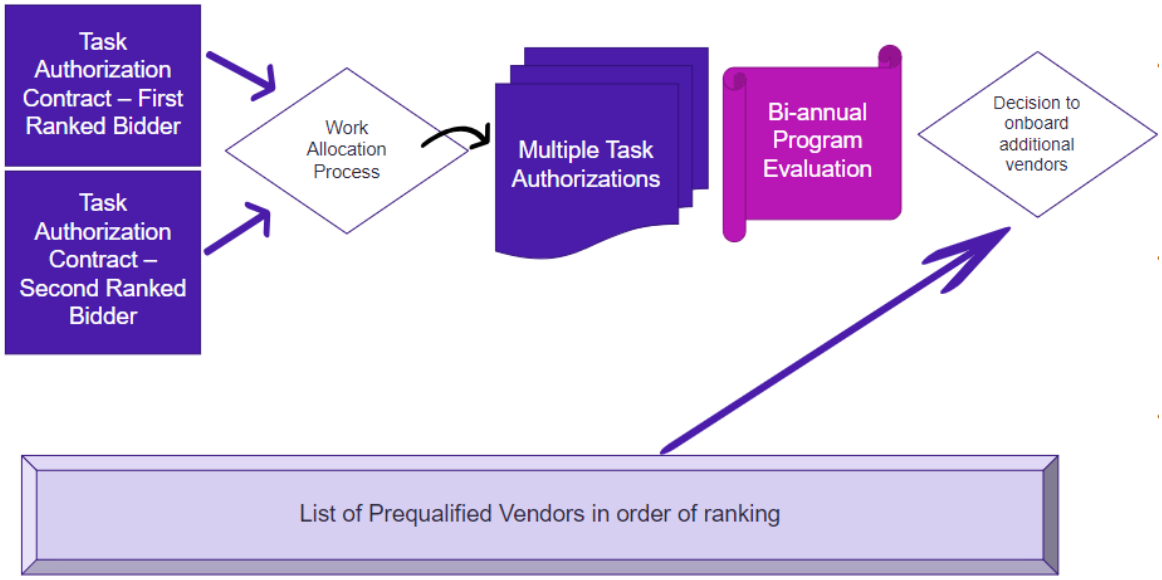
Canada anticipates awarding multiple Task Authorization Contracts.

Canada will not wait for the completion of all activities related to the pre-award stage to start awarding the contracts. As soon as a selected Bidder has completed their obligations and Canada has completed its verifications, Canada may award the contract. Contracts might not be all awarded at the same time; each will be awarded upon having any of the retained Bidders meeting all the pre-award requirements.

Stage 12: Task Authorization

This infographic is a visual representation of the Statement of Challenge task authorization process.

Table 2 – Allocation of Task Authorizations



This solicitation will result in the following:

1) **Contracts:** Up to two Contractors that will be invited to sign a Task Authorization Contract (TAC). Signatories of Task Authorization Contracts will be eligible to sign task authorizations in accordance with Section 6 – Resulting Contract Clauses.

2) **A list of prequalified Contractors** that meet all the requirements of the Final CBS but were not the top 2 ranked bids selected, that could be onboarded in the procurement ecosystem in the upcoming years. Biannually, Shared Service Canada (SSC) will assess vendors' performance, department needs, technology evolution or any other elements and may decide to onboard one or more Contractors on the prequalified list.

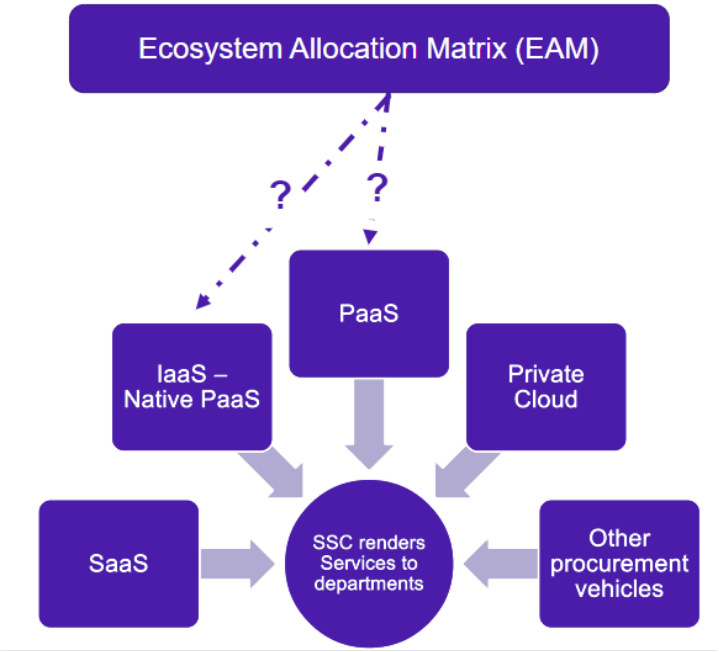
1.5 Task Authorization Contract

Canada intends to structure the contractual agreement as a Task Authorization Contract (TAC). Individual task authorizations (TAs) will be issued against this contract for Cloud services. A contract with Task Authorizations is a method of supply for services under which all of the work or a portion of the work will be performed on an "as and when requested basis" through predetermined conditions including an administrative process involving Task Authorizations.

1.6 Procurement Ecosystem (PE)

- SSC may select one or more procurement vehicles (PV) to render services to departments.
- The decision to select one or more PVs will be informed by an Ecosystem Allocation Matrix (EAM), illustrated below.
- SSC may undertake competition between services from different procurement vehicles (e.g., competition of PaaS: competition of services from IaaS – Native PaaS and PaaS procurement vehicles).
- The Ecosystem Allocation Matrix (EAM) will be disclosed in each solicitation leading to establishing the PVs.
- The EAM may be revised annually in consultation with qualified contractors under the PE.

Table 3 – Procurement Ecosystem



(Note to Bidders: the model of procurement ecosystem is still in discussion and may evolve).

SECTION 2 – INSTRUCTIONS TO BIDDERS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the Challenge-Based Solicitation 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.

Bidders who submit a Bid agree to be bound by the instructions, clauses and conditions of the Challenge-Based Solicitation and accept the clauses and conditions of the resulting Contract.

2.2 Standard Instructions

The SACC 2003 (2023-06-08) Standard Instructions – Goods or Services – Competitive Requirements are incorporated by reference into and form an integral part of this Solicitation, and are amended as follows:

a) At section 03: Standard instructions, clauses, and conditions:

Delete: "Pursuant to the Department of Public Works and Government Services Act, S.C. 1996, c.16."

b) At section 04: Definition of Bidder:

Delete: in its entirety;

Insert: "Bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) that is the originator of the public cloud service in its entirety submitting a bid to perform a contract for goods, services or both. It does not include, the parent, subsidiaries or other affiliates of the bidder, or its subcontractors neither its resellers.

c) At section 05: *Submission of bids*, subsection 4:

Delete: "Bids will remain open for acceptance for a period of not less than 60 days from the closing date of the bid solicitation unless specified otherwise in the bid solicitation."

Insert: "Bids will remain open for acceptance for a period of not less than 180 days from the closing date of the bid solicitation, unless specified otherwise in the bid solicitation."

d) At section 08: Transmission by facsimile or by Canada Post Corporation's (CPC) Connect service:

Delete: in its entirety;

e) At section 09: *Customs clearance*:

Delete: in its entirety;

f) At section 13: Communications – solicitation period:

Delete: "To ensure the integrity of the competitive Bid process, enquiries and other communications regarding the Bid solicitation must be directed only to the Contracting

Authority identified in the Bid solicitation. Failure to comply with this requirement may result in the Bid being declared non-responsive."

Insert: "To ensure the integrity of the Solicitation process, all enquiries regarding this Solicitation must be directed only to the Contracting Authority identified in the Solicitation.

The integrity of the Solicitation process cannot be guaranteed when Bidders seek to raise issues with other departmental representatives; by that, potentially influencing the outcome of an active procurement. As such, Bidders must not engage with any departmental representative other than the Contracting Authority, to raise any issues about this solicitation. This will ensure that issues are raised and addressed in writing and subsequently circulated to all Bidders.

While public servants (who may or may not be involved in this Solicitation) may engage in exchanges on other forums, such as social media, Bidders relying on "found" information do so at their own risk.

Failure to comply with section 13: *Communications – solicitation period* may result in a Bid being declared non-responsive.

2.3 Terms and Conditions of the CBS

SSC Terms and Conditions

Acceptance by Bidders of SSC – RESULTING CONTRACT CLAUSES (Section 6), including the Annex A – Cloud General Terms and Conditions, is a mandatory requirement of this Solicitation.

No modification to the RESULTING CONTRACT CLAUSES (Section 6) included in the Bidder's Bid will apply to the resulting Contract, even though the Bid may become part of the resulting Contract.

Bidders submitting a Bid containing statements implying that the Bid is conditional on modification to these Contract terms and conditions (including all documents incorporated into the Contract by reference) or containing terms and conditions that purport to supersede these Contract terms and conditions will be considered non-responsive. As a result, Bidders with concerns regarding the Contract terms and conditions should raise those concerns in accordance with the clause entitled Enquiries – Solicitation of the CBS.)

No alternative conditions for the proposed cloud services included in the Bidder's Bid, or any terms and conditions in the Bidder's Bid with respect to limitations on liability, or any terms and conditions incorporated into the Bidder's Bid by reference, will apply to the resulting Contract, even though the Bid may become part of the resulting Contract.

Bidder's Additional Cloud Services Terms:

The process for a Bidder to submit Additional Cloud Services Terms is the following:

a) The bidder may, as part of its Prequalification Bid, submit any additional cloud services terms not addressed by SECTION 6 – RESULTING CONTRACT CLAUSES, including Annex A – Cloud General Terms and Conditions, for the Services being offered by the Bidder, i.e., terms that describe how cloud services are provisioned and how they may be

ordered, deployed and used. Proposed supplemental terms must not contradict any term included in SECTION 6 – RESULTING CONTRACT CLAUSES and Annex A – Cloud General Terms and Conditions, and must reflect the same or better terms currently offered to the bidder's commercial customers for the offered services.

b) Bidders should not submit their full standard cloud services terms. Where the Bidder submits their full standard terms, Canada will require that the bidder remove these terms and submit only the terms not already addressed in the resulting contract clauses that the Bidder would like Canada to consider.

c) Should the bidder be one of the highest ranked Bidders invited to sign a task authorization contract, Canada will determine **if Bidder's Additional Cloud Services Terms are acceptable.**

d) **If Bidder's Additional Cloud Services Terms are acceptable,** these supplemental terms will be included as an annex to any resulting task authorization contract, as the last element of the article entitled "**Priority of Documents**."

e) If Canada determines that any proposed cloud services term is unacceptable to Canada, Canada will notify the bidder in writing, and will provide the bidder with an opportunity to remove that provision from its bid or to propose alternate language for consideration by Canada. Canada may set a time limit for the bidder to respond.

f) Unless the additional cloud services terms proposed by the bidder are included as a separate annex to the resulting contract, they will not be considered part of any resulting contract (even if they are part of the bid that is incorporated by reference into the resulting contract). The fact that some additional terms and conditions were included in the bid will not result in those terms applying to any resulting contract, regardless of whether or not Canada has objected to them under the procedures described above.

2.4 Enquiries – Solicitation

Questions and comments about this Solicitation can be submitted in accordance with SACC 2003 (2023-06-08) Standard Instructions – Goods or Services – Competitive Requirements, section 13 *Communications – solicitation period. T*here will be question periods, as follows.

Question Period – Prequalification:

All enquiries are requested to be submitted in writing to the Contracting Authority no later than **5 calendar days before the Prequalification Closing Date**. Enquiries received that do not meet this condition may not be answered prior to the Prequalification Closing Date. Enquiries received after the closing date will not be answered.

Bidders should reference as accurately as possible the numbered item of the Solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature are requested to be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that of the Bidders, so the proprietary nature of the question(s)

is eliminated, and the answer to the enquiry can be provided to all Bidders. Enquiries not submitted in a form that can be provided to all Bidders may not be answered by Canada.

2.5 Contracting Authority

The Contracting Authority is the person designated by that title in the Solicitation, or by notice to the Bidders, to act as Canada's "Contracting Authority" for all enquiries regarding the Solicitation process.

Nadia Kelly

Manager, Cloud Services Team

Shared Services Canada

400 Cooper St, 6th Floor

Ottawa, Ontario K2P 2H8

Email Address: PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca

2.6 Applicable Laws

Any resulting Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in the province of Ontario, Canada.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their Bid, by inserting the name of the Canadian province or territory of their choice. If no change is made, the Bidder acknowledges that the applicable laws specified are acceptable to the Bidder.

2.7 Trade Agreements

This Solicitation is subject to the provisions of the following trade agreement(s):

- Canadian Free Trade Agreement (CFTA)
- Canada-Chile Free Trade Agreement
- Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)
- Canada-Colombia Free Trade Agreement
- Canada-European Union Comprehensive Economic and Trade Agreement (CETA)
- Canada-Honduras Free Trade Agreement
- Canada-Korea Free Trade Agreement
- Canada-Panama Free Trade Agreement
- Canada-Peru Free Trade Agreement
- Canada-Ukraine Free Trade Agreement
- Canada-United Kingdom Trade Continuity Agreement
- World Trade Organization- Agreement on Government Procurement (WTO-GPA)

SECTION 3 BID PREPARATION INSTRUCTIONS - PREQUALIFICATION

3.1 Submission of Written Prequalification Documents by Bidders

By the Prequalification Closing Date and Time noted on the cover page of this Challenge-Based Solicitation, Bidders must submit:

a) The Bid Document 1 – Prequalification Bidding Form that includes the following:

i) Certifications including acceptance of the Rules of Engagement (Attachment 2)

ii) Prequalification Bid that substantiates the Evaluation Criteria detailed in Attachment 1 – Prequalification Evaluation Grid

Bidders are requested to download and save the Prequalification Bidding Form. It is important to use Adobe Reader to open the form, as opening the form directly through an Internet browser or with another PDF reader may result in compatibility issues or errors.

b) Bidder's Additional Cloud Services Terms, if any

3.2 Pre-Bid Compliance Check Process *(OPTIONAL)*

a) **Bidders are invited to submit a Pre-Bid**: Canada invites bidders to submit the following:

i) Bid Document 1 – Prequalification Bidding Form - draft responses to the mandatory requirements.

This is referred to as a "**Pre-Bid**." The submission of a Pre-Bid by any bidder is optional and is not a precondition to submitting a bid on the closing date. Canada will not return Pre-Bids to bidders but will treat Pre-Bids the same way it treats bids, in accordance with Standard Instructions 2003.

b) **How to submit a Pre-Bid**: A bidder may submit a Pre-Bid to the Contracting Authority by sending an email to PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca. When a Pre-Bid is received by email, the Contracting Authority will send an email acknowledgement back to the bidder. If the bidder does not receive an email acknowledgement, the bidder is encouraged to follow up by telephone with the Contracting Authority; or

c) **A Pre-Bid will only be reviewed if submitted by the Pre-Bid Deadline**: Canada will review only Pre-Bids submitted by no later than 11:59 p.m. [insert the date] (the "**Pre-Bid Deadline**"). Canada will review only one Pre-Bid from each bidder (i.e., after receiving feedback, the bidder cannot submit a new version of its Pre-Bid for review).

d) **Canada will provide Feedback on Pre-Bids**: The Contracting Authority will provide confidential feedback, referred to as a Preliminary Evaluation Notice (PEN), to each bidder that has submitted a Pre-Bid by the Pre-Bid Deadline. Canada will normally provide that feedback by email and the bidder is deemed to have received Canada's

feedback at the time it is sent by Canada. Canada is not responsible for any technical delays in the receipt by the bidder of its feedback.

e) **Nature of Canada's Feedback where No Deficiencies identified**: If Canada does not note any deficiencies during its review of a Pre-Bid, Canada will provide the relevant bidder with a "nil" response.

f) **Nature of Canada's Feedback where Deficiencies identified**: If Canada notes deficiencies during its review of a Pre-Bid, Canada will provide written feedback to the bidder indicating any mandatory requirements that Canada have noted:

i) have not been addressed at all.

ii) have not been sufficiently addressed; and

iii) are addressed in such a way that the Pre-Bid would be declared non-compliant if submitted on the closing date.

While Canada will note the reason the Pre-Bid is deficient, Canada will not indicate to the bidder how the deficiency can be corrected.

Once Canada has indicated that a specific mandatory requirement has not been met, Canada is not required to breakdown each way in which the bidder has failed to meet the mandatory requirement. Canada will also not respond to questions about the feedback. If Canada determines that a Pre-Bid is substantially deficient (i.e., there are more than [5] deficiencies identified), Canada reserves the right not to conduct a full review, in which case Canada will identify to the bidder only those deficiencies noted by Canada before it ceased its review. In addressing Canada's feedback, bidders should ensure that the elements of the bid remain consistent following any changes made.

g) **Timing for Providing Feedback**: The time it takes for Canada to provide the feedback will depend on the number of Pre-Bids received and their quality. Canada does not commit to provide its feedback within a specific amount of time. If Canada has not provided feedback with respect to the Pre-Bids at least 5 Calendar days before the scheduled closing date, the closing date will be extended so that all bidders have 5 full Federal Government Working Days (the day of receipt of the feedback is not counted) to finalize their bids prior to the closing date. For example, Canada sends the feedback to the bidders on Monday at 10 a.m. Assuming there are no holidays during this period, the bidder will have Tuesday, Wednesday, Thursday, Friday, and the following Monday to refine its bid. The closing date will be no earlier than the following Tuesday.

h) **Bidders Solely Responsible for Submitting Compliant Bid at Prequalification Bid Closing**: Even if Canada provides feedback regarding a Pre-Bid, the bidder is solely responsible for ensuring that its bid submitted on the closing date is accurate, consistent, complete and fully compliant. Canada does not guarantee that it will identify every deficiency during its review of the Pre-Bid. By submitting a Pre-Bid, the bidder is agreeing that Canada's review is only preliminary, and that Canada will not be responsible in any way for failing to identify any omission, deficiency or non-compliancy during its review of the Pre-Bid.

3.3 Electronic Submission of Bids

All Bidders must submit their Bid by email to PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca by the Prequalification Bid Closing Date.

a) Bidders intending to submit a bid are encouraged to send an email notification to the Contracting Authority indicating their intention to submit a bid by sending an email to PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca.

b) **Email Size**: Bidders should ensure that they submit their submission in multiple emails if any single email, including attachments, will exceed 10 MB . Emails must be received at the above-mentioned email address before the deadline of the Prequalification to be considered part of the Bid submission.

c) **Email title :** Bidders are requested to include the solicitation No. identified on the cover page of this document in the “subject” line of each email forming part of the Bid submission.

d) **Bid submission** : Bidders must submit their submission and be received via email as an attachment to the specified email address PVRCloudServicesRCRs.DCCServicesinfonuagiquesARF@ssc-spc.gc.ca no later than the Prequalification bid closing date as indicated on the cover page. It is the responsibility of the Bidders to ensure that the email submissions is received by SSC. SSC will not be responsible for any undeliverable email submissions.

e) **Responsibility for technical problems**: by submitting a bid, the bidder is confirming it agrees that Canada is not responsible for:

   i) any technical problems experienced by the Bidder in submitting its Bid or attachments that are rejected or quarantined because they contain malware or other code that is screened out by SSC for security reasons; or

   ii) any technical problems that prevent SSC from opening the attachments. For example, if an attachment is corrupted or otherwise cannot be opened or cannot be read, it will be evaluated without that portion of the bid. Bidders will not be permitted to submit substitute attachments to replace any that are corrupt or empty or submitted in an unapproved format.

3.4 Eligibility – Prequalified Bidders

Only Bidders that are qualified at Stage 4 – Prequalification and who remain qualified at the Final CBS Bid Closing Date and Time will be eligible to submit a Bid at the Final CBS stage. Canada reserves the right to re-evaluate any aspect of the qualification of any Bidder at any time during the Solicitation process.

3.5 Submission of Only One Bid

The submission of more than one Bid from any Bidder is not permitted in response to this solicitation. If a Bidder does submit more than one Bid, Canada will ask that Bidder to withdraw all but one of its Bids. If the Bidder does not do so, Canada may choose at its discretion which Bid to evaluate.

SECTION 4 – EVALUATION PROCEDURES AND BASIS OF SELECTION

Bids will be assessed in accordance with the requirements of the Solicitation and the technical and financial evaluation criteria.

There are several steps in the evaluation process, which are described herein. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

An evaluation team composed of representatives of Canada and any of the firms identified on page 4 will evaluate the Bids. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

4.1 Evaluation Procedures – Prequalification (Stage 4 – CURRENT STAGE)

The information submitted in the Bid Document 1 – Prequalification Bidding Form will be evaluated according to Attachment 1 – Prequalification Evaluation Grid.

4.1.1 Basis of Selection for Prequalification

a) To be declared responsive for the Prequalification, a Bid must meet all mandatory criteria in Part A of the Prequalification Evaluation Grid.

b) Bids not meeting all mandatory criteria will be excluded from further participation in the Solicitation process.

4.1.2 Selection of Prequalified Bidders

a) In accordance with 4.1.1 Basis of Selection for Prequalification, Canada will select the 5 highest ranked Bidders for pool formation.

b) If there are fewer than 5 qualified Bidders, all will be selected for pool formation (Stage 4). The score achieved in accordance with Attachment 1 – Prequalification Evaluation Grid will be considered as part of the final selection process (Stage 9) for the Final CBS.

c) If more than one bidder obtains the same rank because of identical scores, then the points obtained for rated criterion R4 of the Prequalification Evaluation Grid will be used to rank the subsequent tied Bid(s) from the highest score to the lowest score. In the case of a second tie, the bidder with the highest number of top-ranked elements from 1 to 9 will be ranked first.

4.2 Evaluation Procedures – FINAL Selection (Stage 9)

Note to Bidders: This section will be further refined after the prequalification. The Final CBS evaluation framework will be discussed with prequalified Bidders and be modified.

If there are 5 or less qualified Bidders at the completion of Stage 4, Canada may decide to remove Stage 8: Demonstration and Feedback and conduct the Selection based on compliance with procedural requirements and a price proposal.

4.3 Number of contracts and qualified vendors permanent list

4.3.1 Contracts: The 2 or 3 highest-ranking responsive Bid(s) (Total Score) will be recommended for Contract award, on the condition that, the second highest-ranking responsive Bid is not within (+/- 1%) of the highest-ranking responsive Bid. In the event that the second highest-ranking responsive Bid is within (+/- 1%) of the highest-ranking responsive Bid, these Bids will be ranked in descending order as follows:

The points obtained for the technical bid evaluation will be used to rank the subsequent tied Bid from the highest score to the lowest score.

4.3.2 Qualified vendors permanent list:

Responsive bids not recommended for contract award will be put on a Qualified Vendor permanent list in their order of rankings.

During the course of the contract, Canada may recommend one or more qualified vendors for Contract award.

4.4 Contract Award

Contract Award is subject to Canada's internal approval processes, which includes a requirement to approve funding in the amount of any proposed Contract(s). Although a Bidder may have been recommended for Contract award, a Contract will only be awarded if internal approval is granted according to Canada's internal approval processes. If approval is not granted, no Contract will be awarded.

Canada will award the contracts only once final agreement is reached on the **Bidder's Additional Cloud Services Terms**, if any. For that reason, the contracts may not be awarded at the same time.

4.5 Media Announcements

The Bidder agrees not to make any media announcements about the award of a Contract without the written consent of the Contracting Authority.

SECTION 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

5.1 Certification requirements

Note to Bidders: This Section is not applicable for the Prequalification.

SECTION 6 – RESULTING CONTRACT CLAUSES

Note to Bidders: the following Contract terms and conditions are intended to form the basis of any Contract(s) resulting from this Challenge-Based Solicitation. Except where specifically set out in the Contract terms and conditions, acceptance by Bidders of all the terms and conditions is a mandatory requirement of this Solicitation.

No modification to the Contract terms and conditions included in the Bidder's Bid will apply to the resulting Contract, even though the Bid may become part of the resulting Contract.

Articles of Agreement

(Note to Bidders: these Articles of Agreement will be refined during the ItR and will be finalized prior to the issuance of the Final CBS).

Series of Contracts

The Contractor acknowledges that this Contract is one of a series of 2 or 3 *[Note to Bidders: this number may be adjusted downward if necessary at the time of award]* contracts awarded as a result of the Challenge-Based Solicitation issued by Shared Services Canada on [insert date] under No. [insert number]. These contracts are included in the IaaS-Native PaaS Procurement Vehicle.

Ecosystem of Procurement Vehicles

The Contractor acknowledges that this IaaS-Native PaaS Procurement Vehicle is one of multiple procurement vehicles for the Hosting contracting Ecosystem.

The Contractor acknowledges that:

- SSC may select one or more procurement vehicles (PV) to render services to departments.
- The decision to select one or more PVs will be informed by the Ecosystem Allocation Matrix (EAM).
- SSC may undertake competition between products from different procurement vehicles (e.g., competition of PaaS: competition of services from IaaS – Native PaaS and PaaS procurement vehicles).
- The EAM will be disclosed in each of the solicitations leading to establishing the PVs.
- The EAM may be revised annually in consultation with qualified contractors under the PE.

Evolving Ecosystem

During the course of the contract, in cases where the technological context will render available innovative services that could help Canada to better resolve the problem identified in the SoC that meet the requirements of this Contract, the Contractor will make those services available on its catalogue at its public price minus GoC discounts.

In cases where the improvement would be provided by a third party (other than the Contractor), Canada may do one of the following:

(1) Invite the highest ranked vendor on the qualified vendors permanent list to sign a task authorization contract and be included in the IaaS-Native PaaS procurement vehicle.

(2) Launch a new solicitation to qualify new Contractors with the ability to help Canada to resolve problems and better address Canada's challenges.

Collaborative Environment:

While Canada recognizes that the contractors issued this series of contracts compete with one another, the Contractor agrees that it will:

(1) except for disclosures required by law, not make any media or other public statements regarding any services rendered or products delivered under this series of contracts by another contractor without the prior consent of the Contracting Authority; and

(2) actively participate in group discussions scheduled by Canada, on the understanding that no contractor is expected to share its intellectual property, confidential information or proprietary information during these sessions.

6.1 Requirement

6.1.1 ***[Cloud Service Provider Name]*** ("**Contractor**") agrees to provide the Cloud Services described in the Statement of Challenge ("**SoC**), and to stand ready to supply Clients with the services described in individual TAs issued by Canada, in accordance with, and at the prices set out in this Task Authorization Contract ("**TAC**") and the relevant Task Authorization (TA), which will be the prices set out in the Contractor's published price list minus committed discounts.

6.1.2 **Client**: Under this TAC, Shared Services Canada ("**SSC**"), is both the Contracting Authority ("**TAC's CA**") and the Technical Authority. This TAC will be used by SSC to provide services to the "**End Users**," which include SSC itself, those government institutions for whom SSC's services are mandatory at any point during the TAC Period or any individual TA Period, and those other organizations for whom SSC's services are optional at any point during either period of time and that chooses to use those services from time to time. SSC may choose to use this TAC for some or all of its Clients and may use alternative means to provide the same or similar services.

6.1.3 **Reorganization of Client**: The Contractor's obligation to provide the Cloud Services will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Government of Canada Client. The reorganization, reconfiguration or restructuring of the Client includes the privatization of any Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the CA or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

6.1.4 **Other Jurisdictions**: Canada reserves the right to allow other Canadian Jurisdictions to use the contract for Cloud Services requirements.

6.1.5 Defined **Terms**: Words and expressions used in this TAC are defined in Annex E.

6.2 Task Authorization (TA)

The Cloud Services or a portion of the Cloud Services to be performed under the Contract will be on an "as and when requested basis" using a Task Authorization.

6.3 Contract Period and Task Authorization Period

6.3.1 The "**Contract Period**" is the entire period of time during which the Contractor is obliged to provide Cloud Services under the TAC, which begins on the date of TAC contract award and ends when Canada ceases to use the contract. This is the period during which Canada may issue TAs.

6.3.2 The "**Task Authorization (TA) Period**" is the entire period of time during which the Contractor is obliged to provide the Cloud Services, which includes:

a) The "**Initial TA Period**," which begins on the date the TA is issued and ends when the Contractor has provided the Cloud Services in accordance with the TA requirements; and

b) any period during which the TA is extended by Canada.

6.3.3 Option to Extend the TA:

The Contractor grants to Canada the irrevocable option to extend the term of the TA under the same terms and conditions, subject to the availability of the same Cloud Services, through a TA amendment issued by the Contracting Authority. The Contractor agrees that, during the extended period of the TA, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

6.4 Task Authorization Process

6.4.1 As more than one contract has been awarded for this requirement, one of the two Contractors will be invited to sign a TA in accordance with the Work Allocation Process (WAP) described under section 6.5.

6.4.2 The Contractor identified by the WAP will receive a request to perform a task. If that Contractor confirms in writing that it is unable to perform the task, the request to perform a task will then be forwarded to the Contractor ranked second. If no contractor can perform the task, Canada reserves the right to acquire the requirement by other means. A Contractor may advise the Technical Authority and the Contracting Authority in writing that it is unable to carry out additional tasks as a result of previous commitments under a TA and no request to perform a task will be sent to that Contractor until that Contractor has given notice in writing to the Technical Authority and the Contracting Authority that it is available to perform additional tasks.

a) The Technical Authority will provide the Contractor with a description of the task using the Task Authorization Form specified in Attachment 1.

b) The resulting Task Authorization (TA) will contain the details of the activities to be performed or services to be rendered and a description of the deliverables. The TA will also include the applicable basis (bases) and methods of payment as specified in the Contract.

c) The Contractor must not commence work until a TA authorized by the Contracting Authority has been received by the Contractor. The Contractor acknowledges that any work performed before a TA has been received will be done at the Contractor's own risk.

6.5 Work Allocation Process

(Note to Bidders: Will be developed during the ItR).

6.6 Multiple Task Authorizations issued

6.6.1 The Contractor acknowledges that:

a) Multiple **Task Authorizations** will be awarded by Canada with respect to Cloud Services.

b) **Competitive Award**: The Contractor acknowledges that the TAC has been awarded as a result of a competitive process.

c) Provided Canada respects the Task Authorization Work Allocation Process described in this document, the Contractor has no rights against Canada with respect to the way in which Canada administers the contracts with other contractors. For example, the Contractor will have no right to bring any claim against Canada as a result of Canada choosing to grant extensions to any other contractor or choosing not to exercise rights or remedies to which Canada may be entitled pursuant to another contract in this series of contracts. If any Task Authorization involves work provided by more than one contractor, the interaction between those contractors or a third-party contractor will be addressed in the Task Authorization.

6.6.2 Responding to Task Authorizations: While the Contractor is not required to respond to Task Authorizations, the Contractor agrees to engage actively in the review of Task Authorization requests and to respond to those for which it can perform the requested tasks.

6.7 Basis of Payment

The Contractor will be paid for the requirement specified in the authorized TA, in accordance with the Basis of Payment.

Canada's liability to the Contractor under the authorized TA must not exceed the L**imitation of Expenditure** specified in the authorized Task Authorization. Applicable Taxes are extra.

6.7.1 For the Commercially Available Public Cloud Services provided under individual TAs, the Contractor will be paid the firm prices applicable to the cloud service(s) selected (e.g., on-demand, subscriptions, prepaid services, etc.), as set out in the Contractor's commercial catalogue less any applicable Government of Canada discounts.

a) Charges for Cloud Services shall not exceed the Contractor's published online pricing for the provisioned Commercially Available Public Cloud Service(s).

The Contractor must provide Canada with the benefit of tiered pricing discounts and volume rebates, where applicable.

i. If there is a price decrease to a Cloud Service already provisioned, the Contractor will apply the price decrease.

ii. The new lower price of the Cloud Service(s) must be applied automatically to the next outstanding payment owed by the Client and will be maintained for the remaining length of the TA, unless a new lower price is made available.

6.7.2 Canada will indicate the payment terms within the TA.

6.7.3 **Service Credits**: If the Cloud Service does not meet the Minimum Availability Level in any given month, Canada will be entitled to claim credits in accordance with the Contractor's commercially available published service level agreement and service credit process.

6.7.4 **Currency**: All native commercially available Cloud Services must be payable in Canadian dollars. In cases where the CSP's commercially available online pricing for non-native services are in US dollars, the CSP must include functionality to allow pricing to be converted to Canadian dollars. The conversion rate must be as favourable as the one offered to the CSP's commercial customers.

6.7.5 **Auto-Renewal Opt Out**: Canada hereby provides notice to the Contractor that, unless otherwise stated in any TA, it opts out of any auto-renewal of the Commercially Available Public Cloud Services.

6.8 Method of Payment

6.8.1 **Method of Payment for On-Demand Services:** Canada will pay in arrears for On-Demand Cloud Services requested by Canada, in accordance with the TA, that have been provisioned and received by Canada, applicable taxes extra. Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment. The Contractor must submit an invoice for each active TA showing all consumption details to support the charges claimed in the invoice.

6.8.2 **Method of Payment for All Subscription Based Services:** Canada will pay in advance for Subscription Based Cloud Services requested by Canada, in accordance with the TA, applicable taxes extra. Canada will make the advance payment to the Contractor for all Subscription-Based Services (both Monthly and Annual) within 30 days after receiving a complete invoice (and any required substantiating documentation), or within 30 days of any date specified in the Task Authorization for making that advance payment, whichever is later.

a) If Canada disputes an invoice for any reason, Canada will pay the Contractor the undisputed portion of the invoice, as long as the undisputed items are separate line items on the invoice and owed. In the case of disputed invoices, the invoice will only be considered to have been received for the purpose of calculating "Interest on Overdue Accounts" once the dispute is resolved.

b) The Contractor acknowledges that this is an advance payment and that payment in advance does not prevent Canada from exercising any or all potential remedies in relation to this payment or any of the Cloud Services, if the Cloud Services were not provided in accordance with the TA.

6.8.3 **Method of Payment for Prepaid Task Authorization with a Maximum Price:** Canada will pay in advance a lump sum from which the Contractor will deduct, monthly in arrears, the cost of the Cloud Services consumed, applicable taxes extra.

a) The terms for advance payment will be for no more than 1 year of service.

b) Where the terms for advance payment are periodic up to 1 year then Canada will indicate within the TA a period of monthly, quarterly or semi-annual payments.

c) Payments in arrears will be made on a period of monthly or quarterly payments.

6.8.4 For each Task Authorization validly issued under the Contract that contains a maximum price:

a) Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment.

b) The Contractor must submit an invoice for each active TA showing all consumption and/or subscription/prepaid details to support the charges claimed in the invoice.

c) Provided that the Contractor makes tools accessible for Clients to monitor consumption and allows them to set thresholds and alerts related to Cloud Services usage and consumption, the Contractor may submit additional invoice(s) for consumption that exceeds the prepaid price.

d) Where services are accepted or terminated outside of the regular billing cycle (e.g., monthly), the Contractor must invoice in accordance with its commercially available published process.

6.9 Disclosure of Greenhouse Gas Emissions and Setting of Reduction Targets.

Canada is committed to achieving net-zero greenhouse gas (GHG) emissions by 2050 in an effort to position Canada for success in a green economy and to mitigate climate change impacts. As a result, the final CBS solicitation may include the following:

i) Evaluation criteria or other instructions in the solicitation of offers or contract documents related to measuring and disclosing your company's GHG emissions;

ii) Requested or required to join one of the following initiatives in order to submit an offer or if awarded a contract:

(A) Canada's Net-Zero Challenge

(B) the United Nations Race to Zero

(C) the Science-based Targets Initiative

(D) the Carbon Disclosure Project

(E) the International Organization for Standardization;

iii) Required to provide other evidence of your company's commitment and actions toward meeting net-zero targets by 2050.

6.10 Engagement with Public Servants:

6.10.1 The Contractor agrees that, unless it has the written consent of the Contracting Authority, it will not send unsolicited emails or other materials to Canadian federal public servants lobbying or otherwise promoting that the Contractor be given more Work or relating to the administration of this Contract or any Task Authorizations issued pursuant to it.

6.10.2 Except as contemplated under a Task Authorization, the Contractor must not discuss the products of any third party, including the other contractors under this series of Contracts in any of its interactions with public servants.

6.11 Authorities

a) **Contracting Authority**

The Contracting Authority for the Contract is:

Name: _____
Title: _____
Phone: _____
Email address: _____

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

b) **Technical Authority**

The Technical Authority for the Contract is (the person will be identified at Contract Award):

Name: _____
Title: _____
Organization: _____
Phone: _____
Email address: _____

The Technical Authority [is the representative of the department or agency 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 Technical Authority; however, the Technical 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.

c) **Contractor's Representative -** (the person will be identified at Contract Award):

Name: _____
Title: _____
Organization: _____
Address: _____
Phone: _____
Email address: _____

6.12 Code of Conduct for Procurement – Contract

The Contractor agrees to comply with the *Code of Conduct for Procurement* and to be bound by its terms for the period of the Contract.

6.13 Priority of Documents for this Contract

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

a) these Articles of Agreement of the Task Authorization Contract (TAC);

b) Annex A – Cloud Terms and General Conditions, Security Obligations, Privacy Obligations

c) Resulting Task Authorization (RTA) Clauses

d) Annex B - Statement of Challenge (SoC)

e) Annex C – Security Requirements Check List (SRCL)

f) Annex D- SRCL Classification Guide

g) Annex E – Defined Terms

h) Annex F - the Contractor's bid dated **[*Date]***, in response to Solicitation Process No. **[*xxxxxx]*** not including any provisions in the bid 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 bid.

i) Annex G – Contractor's Additional Cloud Services Terms Approved by Canada

LIST OF ANNEXES

Annexes that will apply to the resulting contract:

Annex A	**Cloud General Terms and Conditions**
	Schedule 1 - Security Obligations
	Schedule 2 - Privacy Obligations
Annex B	**Statement of Challenge (SoC)**
Annex C	**Security Requirements Check List (SRCL)**
Annex D	**SRCL Classification Guide**
Annex E	**Defined Terms**
Annex F	**Contractor's Additional Cloud Services Terms Approved by Canada**

PREQUALIFICATION DOCUMENTS:

Bid Document 1	**Prequalification Bidding Form**
Attachment 1	**Prequalification Evaluation Grid**
Attachment 2	**Rules of Engagement**

**Note to Bidders: Some of the Annexes and Documents are not included in Stage 4 – Posting of Prequalification CBS. Those documents are currently being developed and will be made available at a later stage.

Annex A Cloud General Terms and Conditions

Table of Contents

1.1 Limitation of Liability

1.1.1 Except as expressly provided in paragraph 1.1.2, the Contractor is liable to Canada for all direct damages it causes in performing or failing to perform the Contract in relation to:

(1) the Contractor's acts or omissions under the Contract as a result of gross negligence, willful misconduct and fraud related to breach of obligations under the Task Authorization Contract (TAC) and breach of intellectual property rights, and;

(2) the Contractor's breach of confidentiality obligations under the Contract, but such limitation does not apply to the disclosure by the Contractor of the trade secrets of Canada or a third party related to information technology.

However, the Contractor is not liable to Canada for indirect, special or consequential damages caused by items 1 and 2 above.

1.1.2 With respect to all direct damages not listed above, the Contractor's maximum liability to Canada is the total estimated cost of the Contract (meaning the dollar amount shown on the first page of the Task Authorization in the block titled "Total Estimated Cost"). Within this maximum, all direct damages not listed above are subject to a maximum of the total amount paid for the Task Authorization in the previous 12 months prior to the liability event.

1.1.3 If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

None of the above limitations apply to damages based on loss of life or injury or claims based on infringement of intellectual property.

1.2 Termination for Convenience

1.2.1 Canada may terminate the TAC and any TA for convenience after writing notice is given to the Contractor or using the termination or cancellation functionality provided through the Contractor's online portal. If the Contract is terminated in part only, the Contractor must continue to provide the Cloud Services that are not affected by the termination notice.

1.2.2 If Canada terminates the TAC and any TA for convenience, the Contractor will be entitled to be paid for the balance owing for any Cloud Services provided pursuant to one or more TAs (less any applicable credits it has applied for and is entitled to receive).

1.2.3 The total of the amounts, to which the Contractor is entitled to be paid under this section, together with any amounts paid, due or becoming due to the Contractor, must not exceed the TA Price. The Contractor will have no claim for damages, compensation, loss of profit, allowance arising out of any termination notice given by Canada under this section except to the extent that this section expressly provides. The Contractor agrees to repay immediately to Canada the portion of any advance payment that is unliquidated on the date of termination.

1.2.4 The termination of the TAC for convenience does not terminate any individual TA for convenience. Any individual TA would be separately terminated for convenience. The termination of the TAC shall not affect or terminate an individual TA entered into prior to the termination date of the TAC, unless the event giving rise to the termination of the TAC results directly from a breach of the Contractor's or Canada's obligations under such TA, in which case such TA shall be terminated in accordance with its terms.

1.3 Termination for Default

The Contracting Authority may terminate the TAC with immediate effect by delivering notice of termination to the Contractor, in the following circumstances:

The Contractor does not meet the ongoing qualification requirements described in this TAC;

1.3.1 The Contractor has breached any of the specific terms and conditions detailed in this TAC or in an individual TA; or

1.3.2 The Contractor becomes bankrupt or insolvent.

1.4 Retrieval of Canada's Data at Termination

At all times during the TAC Period, Canada must have the ability to access and extract all Canada's Data stored in the Service. Upon termination of the entire TAC or one or more TAs, the Contractor must retain Canada's Data stored in the Service for a minimum of 90 calendar days and provide Canada with a limited function account, similar to the GC master account, which provides Canada with the ability to extract its data during that period. Canada must have the ability to securely extract its data and metadata in a machine-readable and usable format acceptable to Canada, at no additional cost if there is termination for default. After the retention period ends, the Contractor must, upon request by Canada, disable Canada's account.

1.5 Ongoing Qualification Requirements and Certifications

1.5.1 The Contractor must continue to meet the qualification requirements and comply with its certifications in its bid as a condition of the TAC, which are subject to verification by Canada during the entire TAC Period and each TA Period. If the Contractor no longer remain qualified, does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, under the default provision of the TAC, to terminate the TAC and one or more TAs for default.

1.5.2 The Contractor must provide any information requested by Canada with respect to whether it continues to meet the ongoing qualification requirements within a reasonable period requested by Canada, not to exceed 15 FGWDs or as otherwise mutually agreed upon.

1.6 Security and Privacy Requirements for Contractors

The security and privacy requirements set out in this Task Authorization Contract apply to and form part of the TAC and each TA and must be maintained at all times during the TAC Period and each TA Period.

1.7 Ongoing Supply Chain Integrity Process

1.7.1 The Parties acknowledge that security is a critical consideration for Canada with respect to this TAC and that ongoing assessment of SCSI will be required with respect to individual TAs throughout the TAC Period.

1.7.2 The parties acknowledge that Canada reserves the right to review the native Cloud Services and third-party marketplace services of any Contractor in whole or in part at any time for supply chain integrity concerns. This acknowledgement does not obligate the Contractor to support the SCSI review.

1.7.3 Throughout the TAC Period and any TA Period, the Contractor must provide to Canada information relating to any data breach of the Contractor's network of which it knows that results in either (a) any unlawful access to Canada's content stored on Contractor's equipment or facilities, or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure or alteration of Canada's content in relation to change of ownership, to the Cloud Services under this TAC, and to any individual TA, that would compromise the integrity, confidentiality, access controls, availability, consistency or audit mechanism of the system or the data and applications of Canada.

1.8 Sub-processors

1.8.1 The Contractor must provide a list of Sub-processors that could be used to perform any part of the Cloud Services in providing Canada with the Cloud Services. The list must include the following information (i) the name of the Sub-processor; (ii) the identification of the scope of activities that would be performed by the Sub-processor; and (iii) the country (or countries) where the Sub-processor would perform the activities required to support the Cloud Services.

1.8.2 The Contractor must provide a list of Sub-processors within ten days of the Task Authorization Contract award date. The Contractor must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processor at least 14 days in advance of providing that Sub-processors with access to Customer Data or Personal Data.

1.9 Change of Control

1.9.1 If Canada determines in its sole discretion that a change of control affecting the Contractor (either in the Contractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada may terminate the TAC on a "no-fault" basis by providing notice to the Contractor within 90 calendar days of receiving the notice from the Contractor regarding the change of control. Canada will not be required to provide its reasons for terminating the TAC 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.

1.9.2 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 Contractor 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 Contractor must, within 30 calendar days of receiving Canada's determination, arrange for another subcontractor, acceptable to Canada, to deliver the portion of the Cloud Services being delivered by the existing subcontractor (or the Contractor must deliver this portion of the Cloud Services itself). If the Contractor fails to do so within this time period, Canada will be entitled to terminate the TAC on a "no-fault" basis by providing notice to the Contractor within 120 calendar days of receiving the original notice from the Contractor regarding the change of control.

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

1.9.4 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 Contractor or subcontractor, as the case may be; that is, Canada does not have a right to terminate the TAC pursuant to this Article where the Contractor or subcontractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner.

1.10 Insurance Requirements

The Contractor is responsible for deciding if insurance coverage is necessary to fulfill its obligation under the TAC or any individual TA and to ensure compliance with any applicable law. Any insurance acquired or maintained by the Contractor is at its own expense and for its own benefit and protection.

1.11 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Canada and in the province of Ontario.

1.12 Invoicing Instructions

1.12.1 The Contractor must submit invoices for each TA issued under the TAC. All invoice pricing and payment must be in Canadian dollars.

1.12.2 The Contractor's invoice must indicate the Cloud Services and the quantity for which it is invoicing, with corresponding unit prices, in accordance with the Basis of

Payment, and the extension of totals of services provided. Invoices must also include the date, TA number, Procurement Business Number and financial code(s).

1.12.3 By submitting invoices (other than for any items subject to an advance payment), the Contractor is certifying that the Cloud Services have been provided, and charges calculated, in accordance with the TA.

1.12.4 The Contractor must apply any applicable Service Credits owing to Canada following the submission of a valid claim in accordance with the Contractor's commercially available published process, to the TA invoice that follows the month after the Service Credits accrue under that TA.

1.12.5 Applicable Taxes must be specified on all invoices as a separate item, along with corresponding registration numbers from the tax authorities.

1.12.6 The Contractor must provide the original of each invoice to the End User. On request, the Contractor must provide a copy of any invoices requested by the Contracting Authority.

1.13 Interest on Late Payments

Canada's standard payment period is 30 days. Canada will pay to the Contractor simple interest at the Average Rate (the simple arithmetic mean of the Bank Rates in effect at 4:00 p.m. Eastern Time each day during the calendar month immediately before the month in which payment is made) plus 3 percent per year on any amount that is overdue, from the date that amount becomes overdue until the day before the date of payment, inclusive, provided Canada is responsible for the delay in paying the Contractor.

1.14 Foreign Nationals

The Contractor must comply with Canadian immigration requirements applicable to foreign nationals entering Canada to work temporarily in fulfillment of the TAC or any individual TA. If the Contractor wishes to hire a foreign national to work in Canada to fulfill the TAC or TA, the Contractor should immediately contact the nearest Service Canada regional office to enquire about Immigration, Refugees and Citizenship Canada's requirements to issue a temporary work permit to a foreign national. The Contractor is responsible for all costs incurred as a result of non-compliance with immigration requirements.

1.15 Limitation of Expenditure

1.15.1 Canada's total liability to the Contractor under each individual authorized TA issued by the Contracting Authority must not exceed the amount set out in the TA, applicable taxes included, including any revisions issued by the Contracting Authority.

1.15.2 No increase in the liability of Canada will be authorized or paid to the Contractor unless an increase has been approved, in writing, by the Contracting Authority.

1.15.3 The Contractor must provide reporting capabilities within its service that allow the End User to assess the adequacy of this sum and determine whether they need to reduce usage or increase funding in order to permit provision of the Cloud Services within budget.

Security Obligations

At the contracting stage, the Contractor will need to fully satisfy security requirements up to and including Protected B / High Value Assets (HVA) as defined in Canadian Center for Cyber Security (CCCS) guidance, unless otherwise specified. The language and full list of requirements will be further refined during one of the Invitation to Refine (stage 5).

Appendix A – Schedule 1 – Security Obligations for Commercial Cloud Services (up to and including Protected B – High Value Assets Overlays)

1. General

1.1 *Purpose*

The purpose of this Schedule is to set forth the obligations of the Contractor relating to the proper management of Canada's Data, including protection from unauthorized modification, access or exfiltration, in accordance with the Agreement, this Schedule, and the Contractor's Security Measures (collectively, the "**Security Obligations**").

1.2 *Flow-Down of Security Obligations*

The obligations of the Contractor contained in these Security Obligations must be flowed down by the Contractor to any Sub-processors and/or Subcontractors to the extent applicable.

1.3 *Change Management*

(1) The Contractor must, throughout the Contract, take all steps required to update and maintain the Security Requirements as needed to comply with the security best practices and industry standards as set forth in this Schedule.

(2) The Contractor must advise Canada of all changes that materially degrades or may have an adverse effect to the Cloud Services offerings in this Contract, including technological, administrative or other types of changes or improvements. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgments

The parties acknowledge that:

(1) Canada's Data is subject to these Security Obligations.

(2) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Canada's Data.

(3) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Cloud Services Personnel to access Canada's Data prior to the implementation of the Security Requirements as required under this Schedule on or before Contract Award.

(4) Security Obligations apply to **Commercial Cloud Services** (up to and including Protected B / High Value Assets (HVA) as defined in Canadian Center for Cyber Security (CCCS) guidance), unless otherwise specified.

3. Securing Canada's Data

(1) The Contractor must protect Canada's Data from unauthorized access, modification, or exfiltration. This includes implementing and maintaining appropriate technical and organizational security measures including information security policies, procedures, and security controls to preserve the confidentiality, integrity, and availability of Canada's Data.

4. Roles and Responsibilities for Security

(1) The Contractor must clearly delineate the roles and responsibilities for the security controls and features of the Cloud Services between the Contractor and Canada. This includes, at a minimum, the roles and responsibilities for: (i) account management; (ii) boundary protection; (iii) asset and information system back-up; (iv) incident management; (v) System monitoring; and (vi) vulnerability management.

(2) The Contractor must provide to Canada an up-to-date document that delineates the roles and responsibilities: (i) at contract award; (ii) on an annual basis; (iii) when there are significant changes to such roles and responsibilities as a result of a Change to the Cloud Services; or (iv) upon request of Canada.

5. Cyber Security Program

(1) The Contractor must maintain a cyber security program designed to protect the confidentiality, integrity and availability of the Information Systems which includes Contractor Services, Sub-processors and/or Subcontractors processing and storing the Canada's Data.

(2) The cyber security program must be based on the Contractor's Risk Assessment and must be designed to perform the following core cyber security functions:

(a) identify and assess internal and external cyber security risks that may threaten the security or integrity of Canada's Data stored on the Contractor's Information Systems

(b) use defensive infrastructure and the implementation of policies and procedures to protect the Contractor's Information Systems, and the Canada's Data stored on those Information Systems, from unauthorized access, use or other malicious acts;

(c) detect cyber security events;

(d) respond to identified or detected cyber security events to mitigate any negative effects;

(e) recover from cyber security events and restore normal operations and services; and

(f) fulfill applicable regulatory reporting obligations.

(3) The Contractor must designate a qualified individual (e.g., Chief Information Security Officer, Company Security Officer, etc.) responsible for overseeing and implementing the Contractor's cyber security program and enforcing its cyber security policy. This designated individual must:

(a) retain responsibility for compliance with the Security Obligations listed in this document;

(b) report compliance with the Security Obligations in writing at least annually to Canada;

(c) report on cyber security risks to the Contractor and to Canada's Data; and

(d) report on the overall effectiveness of the Contractor's cyber security program.

(4) All documentation and information relevant to the Contractor's cyber security program shall be made available to Canada upon request.

6. Cyber Security Policy

(1) The Contractor must implement and maintain a written policy or policies, approved by a Senior Officer or the Contractor's board of directors or equivalent governing body, setting forth the Contractor's policies and procedures for the protection of its Information Systems and data stored on those Information Systems. The cyber security policy shall be based on an organizational Risk Assessment and address the following areas to the extent applicable to the Contractor's operations:

(a) Information security;
(b) Data governance and classification;
(c) Asset inventory and device management;
(d) Access controls and identity management;
(e) Business continuity and disaster recovery planning and resources;
(f) Systems operations and availability concerns;
(g) Systems and network security;
(h) Systems and network monitoring;
(i) Systems and application development and quality assurance;
(j) Physical security and environmental controls;
(k) Customer data privacy;
(l) Supply chain risk management including vendor and third-party service provider management;
(m) Risk assessment;
(n) Security awareness and training; and
(o) Incident response.

7. Risk Assessment

(1) The Contractor must conduct a periodic Risk Assessment of the Contractor's Information Systems sufficient to inform the design of the cyber security program as required by this Part. Such Risk Assessment must be updated as reasonably necessary to address changes to the Contractor's Information Systems, while continuing to meet the Security Obligations as listed in this document. The Contractor's Risk Assessment must allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Contractor's business operations related to cyber security, Canada's data collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Canada's data and Information Systems.

(2) The Risk Assessment must be carried out in accordance with written policies and procedures and must be documented. Such policies and procedures must include:

(a) criteria for the evaluation and categorization of identified cyber security risks or threats facing the Contractor;

(b) criteria for the assessment of the confidentiality, integrity, security and availability of the Contractor's Information Systems and Canada's data, including the adequacy of existing controls in the context of identified risks;

(c) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cyber security program will address the risks; and

(d) regular cyber security awareness training for all personnel that is updated to reflect risks identified by the Contractor in its Risk Assessment.

8. Third-Party Assurance: Certifications and Reports

(1) The Contractor must ensure that Canada's Data, Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations are secured with appropriate security measures that comply with the requirements set forth the Contractor's security practices and policies.

(2) The Contractor must demonstrate that the measures comply 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 27001:2022 Information security, cybersecurity and privacy protection -- Information security management systems – Certification achieved by an accredited certification body (or subsequent versions); 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 (or subsequent versions); 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.

(3) Each certification or audit report provided must: (i) identify the legal business name of the Contractor or applicable Sub-processor; (ii) identify the Contractor's or Sub-processor's certification date and the status of that certification; (iii) identify the services included within the scope of the certification report. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

(4) Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor and provide Canada with supporting evidence of the remediation measures taken or confirmation from the auditor that issues have been remediated to the satisfaction of the auditor.

(5) Each SOC 2 Type II audit report must have been performed within the 12 months prior to the start of the contract. A bridge letter may be provided to demonstrate that the Contractor is in process of renewal where there is a gap between the service organization's report date and the user organization's year-end (i.e., calendar or fiscal year-end).

(6) The Contractor is expected to maintain its certification of ISO 27001, ISO 27017, and/or SOC 2 Type II as applicable for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

9. Auditing Compliance

(1) The Contractor must ensure that privacy and security audits of the security of the computers, computing environment and physical data centers that it uses in processing and protecting Canada's Data are conducted as follows :

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by independent, third-party auditors that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(2) Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings by the third-party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

(3) Upon request of Canada, additional supplementary evidence from the Contractor, including system security plans, designs, or architecture documents that provide a comprehensive system description, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 8 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications. This includes the situation where the Contractor is a SaaS or PaaS provider using physical data centers that are provided by a third-party IaaS provider.

10. Cloud Service Provider (CSP) IT Security Assessment

(1) The Contractor must hire a FedRAMP authorized Third Party Assessment Organization (3PAO) for participation in the IT Security Assessment process.

(2) The Contractor, through the assistance of the retained 3PAO, must demonstrate compliance with the security requirements selected in the

(a) CCCS Medium profile for Cloud (Protected B), also referred to as Annex B CCCS MEDIUM Cloud Profile Recommendations, for the scope of the Cloud Services provided by the Contractor; and

(b) CCCS Protected B High Value Asset overlay, for the scope of the Cloud Services provided and identified as capable by the Contractor.

(3). Compliance will be assessed and validated through the CCCS CSP Information Technology (IT) Security Assessment Process The Contractor must demonstrate that they completed the process by providing the following documentation:

(a) Most recent completed assessment report provided to Canada; and

(b) Most recent summary report provided to Canada.

(4). Canada reserves the right to request evidence of compliance set forth in the security obligations, to assess compliance, and where applicable, to direct the remedy (e.g., enhance security controls) for the operation of the Contractor Services.

(5). It is the continuous obligation of the Contractor of the proposed Cloud Services to notify GC procuring department when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

(6). The Contractor should contact the procuring GC department for any additional information related to the CSP IT Assessment Program.

11. Data Protection

(1) The Contractor must:

(a) Implement encryption of data at rest for the Cloud Services hosting Canada's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with *Section 17 - Cryptographic Protection*.

(b) Transmit Canada's Data in a secure manner including ability for the GC to implement encryption for data in transit for all transmissions of Canada's Data, in accordance with *Section 17 - Cryptographic Protection* and *Section 25- Network and Communications Security*.

(2) The Contractor must:

(a) Implement security controls that restricts administrative access to Canada's Data and Systems by the Contractor and provides the ability to require the written approval of Canada before the Contractor can access Canada's Data to perform support, maintenance or operational activities.

(b) Take reasonable measures to ensure that Contractor Personnel do not have standing or ongoing access rights to Canada's Data, and access is restricted to Contractor Personnel with a need-to-know, including resources that provide technical or customer support, based on approval from Canada.

(c) Implement security controls that restricts the unauthorized use of artificial intelligence tools accessing Canada's data.

(3) The Contractor must not make any copies of databases or any part of those databases containing Canada's Data outside of regular service resilience capabilities and within approved regional spaces or zones within Canada.

(4) The Contractor must not move or transmit approved copies outside of agreed upon service regions except when written approval is obtained from Canada.

(5) Upon request of Canada, the Contractor must provide Canada with a document that describes all additional metadata created from Canada's Data.

12. Data Segregation

(1) The Contractor must implement controls to ensure appropriate segregation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit, and throughout all aspects of the Cloud Services and Contractor Infrastructure's functionality and system administration. This includes implementing access controls and enforcing appropriate logical or physical segregation to support:

(a) The separation between Contractor's internal administration from resources used by its customers;

(b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another; and

(c) (For IaaS) Ability for the GC to support isolation within GC-managed tenant environment.

(2) Upon request of Canada, the Contractor must provide Canada with a document that describes the approach for ensuring appropriate segregation of resources such that Canada's Data are not co-mingled with other tenant data, while in use, storage or transit.

13. Data Location

(1) The Contractor must have the ability to store and protect Canada's Data, at rest, including data in back-ups or maintained for redundancy purposes. This includes the ability to isolate data in Canada in approved data centers. An approved Data Centre is defined as the following:

(a) A data centre that meets all security requirements and certifications identified in *Section 33 for Physical (Data Centre / Facilities) Security*;

(b) Ensures the infeasibility of finding a specific customer's data on physical media; and

(c) Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with *Section 17 - Cryptographic Protection*.

(2) The Contractor must certify that the delivery and provisioning of Cloud Services under this contract is from countries within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm) or the European Union (EU) (https://europa.eu/european-union/about-eu/countries_en), or from countries with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(3) The Contractor must ensure that data about Canada or Canada's citizens or residents – data that is classified at a Protected B level of sensitivity – is collected, processed, and/or stored within the geographical boundary of Canada.

(4) Prior to transferring data about Canada or Canada's citizens or residents outside of Canada for specific processing purposes (e.g. detection of anomalous activity, threat analysis), the Contractor must first:

(a) Obtain agreement from Canada, following which the Contractor must handle the data appropriately, and applies comparable safeguards to achieve similar level of protection as stipulated herein; and

(b) Certify that the delivery and provisioning of Cloud Services under this contract is from countries within the North Atlantic Treaty Organization (NATO) (https://www.nato.int/cps/en/natohq/nato_countries.htm) or the European Union (EU) (https://europa.eu/european-union/about-eu/countries_en), or from countries

with which Canada has an international bilateral industrial security instrument. The Contract Security Program (CSP) has international bilateral industrial security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(c) Canada must be offered an option to opt-out from using a service that is offered by the Contractor and delivered from outside of Canada, and in which case, be offered a similar service offering that is delivered from within Canada when requested to do so.

(d) The Contractor must not store the data outside of Canada.

(5) The Contractor must not use or disclose the information for another purpose. Thus, a transfer of data for processing must be for a purpose for which the information was originally collected and agreed to by Canada.

(6) The Contractor must have the ability for Canada to isolate Canada's Data hosted in Cloud Services in data centers that are geographically located in Canada.

(7) Upon request of Canada, the Contractor must:

(a) Provide the GC with an up-to-date list of the physical locations, including city, which may contain Canada's Data for each data centre that will be used to provide the Cloud services; and

(b) Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

(8) It is the continuous obligation of the Contractor of the proposed Cloud Services to provide written notification to Canada when there are updates to the list of physical locations which may contain Canada's Data.

14. Data Transfer and Retrieval

(1) The Contractor must provide the capability including tools and services that allow Canada to:

(a) Extract all online, nearline, and offline Canada's Data, including, but not limited to, databases, object and file storage, system configurations, cloud activity logs, source code hosted in a Canada code repository, and network configurations such that any Canada End User can use these instructions to migrate from one environment to another environment; and

(b) Securely transfer all Canada's Data, including content data and associated metadata, in a machine-readable and usable format, including CSV format, and in accordance with the Library and Archives Canada Guidelines on File Formats for Transferring Information Resources of Enduring Value (https://library-archives.canada.ca/eng/services/government-canada/information-

disposition/guidelines-information-management/pages/guidelines-file-formats-enduring-value.aspx).

15. Data Retention

(1) The Contractor must retain data for the life of the contract on based on GC-approved retention period, and in accordance with Library and Archives General Valuation Tools (https://library-archives.canada.ca/eng/services/government-canada/information-disposition/generic-valuation-tools/Pages/generic-valuation-tools.aspx). This includes Canada's data in structured and unstructured format.

(2) The Contractor must dispose of Canada's data as per *Section 16 - Data Disposition and Returning Records to Canada* when it meets the end of the retention period.

16. Data Disposition and Returning Records to Canada

(1) The Contractor must securely erase, purge, dispose or destroy resources (e.g. equipment, data storage, files, and memory) or devices that may contain Canada's data and ensure that previously stored data cannot be re-instantiated from system or devices.

(2) The Contractor must securely dispose or reuse resources (e.g. equipment, data storage, files, and memory) that contain Canada's Data and ensure that previously stored data cannot be accessed by other customers after it is released. This includes all copies of Canada's Data that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following: (i) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Communications Security Establishment (CSE) guidance on IT media sanitization (ITSP.40.006) (https://www.cyber.gc.ca/en/guidance/it-media-sanitization-itsp40006#defn-clearing). Upon request of Canada, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

(3) The Contractor must provide Canada with written confirmation that demonstrates successful erasing, purging or destruction of all resources, as appropriate, and an ability to prevent re-instantiation of any removed or destroyed system, capability (software or process), data, or information instances once Canada discontinues its use of the Cloud Services.

17. Cryptographic Protection

The Contractor must:

(1) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with CSE-approved cryptographic algorithms and cryptographic parameter sizes, key lengths and key crypto periods as specified in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information" (ITSP.40.111) (https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111) and "Guidance on Securely Configuring Network Protocols"(ITSP.40.062)(https://www.cyber.gc.ca/en/guidance/guidance-securely-

configuring-network-protocols-itsp40062) and remain consistent with any subsequent versions published on https://cyber.gc.ca/;

(2) Use CSE-approved cryptographic algorithms that have been validated by the Cryptographic Algorithm Validation Program (CAVP) (https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program), with cryptographic parameter sizes and key lengths, as specified in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information" (ITSP.40.111) (https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111) and remain consistent with any subsequent versions published on https://cyber.gc.ca/;

(3) Ensure that the use of cryptographic algorithms, cryptographic parameter sizes, key lengths and crypto periods are configurable and can be updated within protocols, applications and services to be consistent with transition guidance in time to meet specified transition dates in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B" (ITSP.40.111) (https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111) and "Guidance on Securely Configuring Network Protocols" (ITSP.40.062) (https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) and remain consistent with any subsequent versions published on https://cyber.gc.ca/. Contractors should support the transition to quantum-safe cryptography in accordance with the guidance in ITSP.40.111 and ITSP.40.062 and their subsequent versions.

(4) Ensure that Cryptographic Module Validation Program (CMVP)-validated Cryptographic Modules are used when cryptography is required, and are implemented, configured, and operated in in accordance with the cryptographic module security policy listed on the CMVP-validated modules list (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules), in an either approved or an allowed mode to provide a high degree of certainty that the CMVP-validated cryptographic module is providing the expected security services in the expected manner; and

(5) Ensure that any cryptographic modules in use have an active, current, and valid CMVP certification. CMVP-validated products will have certificate numbers listed on the CMVP-validated modules list (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules).

(6) The cryptographic modules should be configured and operated in an approved or allowed mode in accordance with the CMVP-published security policy.

(7) Support cryptographic agility such that the protection of data in transit or at rest can remain current with cryptographic protection recommendations from CSE/CCCS, including the use of new standards to mitigate the quantum computing threat.

18. Key Management

(1) The Contractor must ensure that the CSP master key or root keys used for deriving other keys are generated and managed through secure and approved FIPS 140-validated processes for key generation, distribution, storage, and lifecycle management.

(2) The Contractor must provide Canada with a key management service aligned with CCCS Guidance on Cloud Service Cryptography (ITSP.50.106) (https://cyber.gc.ca/en/guidance/guidance-cloud-service-cryptography-itsp50106) and their subsequent versions published on https://cyber.gc.ca/, that includes:

(a) Ability to securely import GC generated encryption keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process and store them in a Contractor-managed dedicated HSM for Canada.

(b) Definition and application of specific policies that control how keys can be used;

(c) Protection of access to the key material including prevention from Contractor access to the key material in unencrypted fashion;

(d) Ability to audit all events related to key management services, including Contractor access for Canada's review;

(e) Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys; and

(f) Ability to delegate key use privileges for use by the Cloud Services used for the GC managed services.

(3) The Contractor should provide a key management capability that supports interoperability and access to GC-controlled encryption keys stored in a GC-managed on-premise HSM infrastructure.

19. Endpoint Protection

(1) The Contractor must implement, manage, and monitor security-hardened endpoints with active host-based protections to prevent against malware, attacks and misuse in accordance with industry recognized configuration guidelines such as those found in NIST 800-123 (Guide to General Server Security), the Center for Internet (CIS) Benchmarks or an equivalent standard approved by Canada in writing.

(2) The Contractor must ensure media containing organization data on digital and non-digital media must be protected by cryptographic mechanism to protect the confidentiality and integrity of this information.

20. Secure by Design and Secure Development

(1) The Contractor must implement a software and system development lifecycle as part of a secure by design approach that applies information system security engineering principles

throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as (i) NIST SP 800-160 Vol. 2 Rev. 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, (ii) ISO/IEC 27034-1:2011 - Information technology — Security techniques — Application security — Part 1: Overview and concepts, (iii) CCCS Annex 2 - Information system security risk management activities (ITSG-33), (iv) SAFECode, (v) CISA Principles and Approaches for Security by Design, or (vi) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented software and system development lifecycle approach and process.

21. Identity and Access Management

(1) The Contractor must have the ability for Canada to support secure access to Cloud Services including ability to configure:

(a) Phishing-resistant multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;

(b) Role-based access;

(c) Access controls on objects in storage; and

(d) Granular authorization policies to allow or limit access.

(2) The Contractor must have the ability to establish organization-wide defaults to manage tenant-wide policies.

22. Federation

(1) The Contractor must have the ability for Canada to support federated identity integration including:

(a) Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 (or subsequent versions) and OpenID Connect 1.0 (or subsequent versions) where the End User credentials and authentication to cloud services are under the sole control of Canada; and

(b) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding Cloud Service user account(s).

23. Privileged Access Management

(1) The Contractor must:

(a) Implement access control policies and procedures that address onboarding, off-boarding, transition between roles, regular access reviews to identify excessive privileges, limitations and usage control of administrator privileges;

(b) Manage and monitor privileged access to the Cloud Services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services;

(c) Restrict and minimize access to the Cloud Services and Canada's Data to only authorized devices and End Users with an explicit need to have access;

(d) Enforce and audit authorizations for access to the Cloud Services and Canada's Data;

(e) Constrain all access to service interfaces that host Canada's Data to uniquely identified, authenticated and authorized End Users, devices, and processes (or services);

(f) Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(g) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(h) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Canada's Data;

(i) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;

(j) Adhere to the principles of least privilege and need-to-know when granting access to the Cloud Services and Canada's Data;

(k) Use security-hardened endpoints (e.g. computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g. dedicated endpoint that does not have Internet browsing or open email access) to provide support and administration of Cloud Services and Contractor Infrastructure;

(l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and

(m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring privileged access of the Cloud Services.

24. Remote Management

(1) The Contractor must manage and monitor remote administration of the Contractor's Cloud Service that are used to host GC services and take reasonable measures to:

(a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);

(b) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with *Section 17- Cryptographic Protection*;

(c) Route all remote access through controlled, monitored, and audited access control points;

(d) Expeditiously disconnect or disable unauthorized remote management or remote access connections;

(e) Authorize remote execution of privileged commands and remote access to security-relevant information.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's approach and process for managing and monitoring remote administration of the Cloud Services.

25. Network and Communications Security

(1) The Contractor must:

(a) Provide the ability for Canada to establish secure connections to the Cloud Services, including providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;

(b) Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CCCS's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062configuring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111);

(c) Use correctly configured certificates within the TLS connections in accordance with CCCS's ITSP.40.062 Guidance on securely configuring network protocols.

(https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062)

(d) Provide the ability for Canada to implement network access controls and security rules that restrict access to only authorized devices and network locations to Canada resources.

(e) Provide the ability for Canada to implement dedicated or private connections to its data centres and supported for sensitive workloads that may require such.

(f) Provide tools and capabilities to assess the effectiveness of security controls and provide visibility into the enforcement of security controls across the data transit path using technologies such as activity logs and reporting.

(g) Validate the security posture, uniquely identify, and authenticate requests before establishing a network connection to the customer organization's tenant or cloud resources.

(h) Design and implement operational measures to ensure software, hardware and network communications systems support redundant and resilient services to withstand against disruptions, hardware failures, and cyber destructive events.

26. Logging and Auditing

(1) The Contractor must implement log generation and management practices and controls for all Cloud Service components that store or process Canada's Data, and that conform with industry standards and best practices, such as those found in NIST 800-92 (Guide to Computer Security Log Management), or an equivalent standard approved by Canada in writing. Upon request of Canada, the Contractor must provide a document that describes the Contractor's documented log generation and management practices and controls.

(2) The Contractor must provide the ability for Canada to centrally manage and configure content to be captured in audit records from multiple components (e.g. network, data, storage, compute, etc.) from the Cloud Services consumed by Canada, to enable Canada to perform security monitoring, reporting, analysis, investigation and implementation of corrective actions, as required. This includes the ability for Canada to:

(a) log and detect audit events such as (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, (vi) deletion of data, and in accordance with Canada's Event Logging Guidance (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/event-logging-guidance.html);

(b) ensure that audit events minimize the exposure of sensitive data such as Personal Information with appropriate privacy preserving techniques and safeguards, in alignment with *Section 17 - Cryptographic Protection*;

(c) record in logs (or log files) audit events that are time synchronized and timestamped in coordinated universal time (UTC) and protected from unauthorized access, modification, or deletion while in transit and at rest;

(d) provide real-time alerts of failed audit events to personnel with the authority to address the failed audit events; and

(e) separate Security Incidents and logs for different Canada accounts to enable Canada to monitor and manage events within its boundary that are affecting its instance of an IaaS, PaaS or SaaS Cloud Service provided to it by the Contractor or a Sub-processor.

(3) The Contractor must provide the ability for Canada to export security events and logs using standardized reporting interfaces, protocols, and data formats (e.g. Common Event Format (CEF), syslog, or other common log formats) and APIs that support log data remote retrieval (e.g. via a database interface using SQL, etc.) for the Cloud Services it consumes, in support of GC operations including monitoring of the Cloud Services and for e-discovery and legal holds.

(4) For SaaS, the Contractor must provide Application Programming Interface(s) (APIs) that provide the ability to:

(a) Inspect and interrogate data at rest in SaaS applications;

(b) Export security event logs for the Solution(s); and

(c) Assess events such as user access and behaviour, administrator access and behaviour, and changes to third-party API access, stored in SaaS application logs.

27. Continuous Monitoring

(1) The Contractor must continually manage, monitor, and maintain the security posture of Contractor Infrastructure and Service Locations hosting Canada's Data throughout the contract, and ensure that the Cloud Services provided to Canada are in a manner that complies with these Security Obligations. As part of this obligation, the Contractor must:

(a) Actively and continuously monitor threats and vulnerabilities to Contractor Infrastructure, Service Locations, or Canada's Data;

(b) Implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, Canada's data by such authorized users.

(c) Conduct regular vulnerability scans and penetration testing of the Contractor Infrastructure and Service Locations, with the aim of identifying deficiencies and remediations in order to prevent unauthorized access to sensitive information, circumvention of access controls and privilege escalation, and exploitation of vulnerabilities to gain access to systems or information.

(d) Undertake best efforts to prevent attacks through security measures such as denial of service protections;

(e) Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;

(f) Identify unauthorized use and access of any Cloud Services, data and components relevant to Canada's IaaS, PaaS or SaaS Cloud Service;

(g) Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Cloud Services or libraries that the Cloud Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;

(h) Respond, contain, and recover from threats and attacks against the Contractor Cloud Services; and

(i) Where required, take proactive countermeasures, including taking both pre-emptive and responsive actions, to mitigate threats.

(2) The Contractor's Cloud Services must allow for GC application data (for IaaS, PaaS and SaaS) and GC network traffic (for IaaS and PaaS) of cloud hosted GC services to be copied and forwarded to a predetermined location (in the cloud or on GC premises).

(3) For SaaS, the Contractor's Cloud Services must allow Canada to deploy and operate security software to perform advanced monitoring and mitigations of cyber threats for Canada's Cloud Services for Canada managed components only.

28. Security Incident Management

(1) The Contractor must:

(a) Establish and maintain a security operations center (SOC) capability that operates within the organization's defined time of operation and service model e.g. 24 x 7 service coverage.

(b) Establish and maintain a cyber incident response team that can be deployed by the CSP within the organization's expected service targets.

(2) The Contractor Security Incident response process for the Cloud Services must encompass IT security incident management lifecycle and supporting practices for preparation, detection, analysis, containment, and recovery activities. This includes:

(a) A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP 800-61 Rev.2 Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html); or (iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.

(b) Documented processes and procedures of how the Contractor will identify, respond, remediate, report, and escalate Security Incidents to Canada, including: (i) the scope of the information security incidents that the Contractor will report to Canada; (ii) the level of disclosure of the detection of information security incidents and the associated responses; (iii) the target timeframe in which notification of information security incidents will occur; (iv) the procedure for the notification of information security incidents; (v) contact information for the handling of issues relating to information security incidents, in alignment with the reporting procedures outlined in the GC CSEMP (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html), and (vi) any remedies that apply if certain information security occur.

(c) Ability for the Contractor to support Canada's investigative efforts for any compromise of the users or data in the service that is identified.

(d) Allows only designated, pre-authorized representatives of Customer (e.g. Canadian Centre for Cyber Security, or other GC-approved organizations) authorized by the Technical Authority:

(i) to request and receive discrete access and information associated with Customer's Data (user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
(ii) the ability for Customer to track the status of a reported information security event.

(e) Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and conforms to industry standards and best practices including ISO 22095:2020 Chain of custody — General terminology and models (https://www.iso.org/standard/72532.html) including proper forensic procedures and safeguards for:

(i) the maintenance of a chain of custody for both the audit information, and

(ii) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.

(3) Within ten days of the effective date of the Contract, the Contractor must provide a document that describes the Contractor's Security Incident Response Process including contact information. This process including contact information must remain up-to-date, and at a minimum, be validated on an annual basis, and be approved by Canada.

(4) The Contractor must:

(a) Work with Canada's Security Operations Center(s) (e.g. GC SOC, Departmental IT Security Teams) and GC CSEMP Primary Stakeholders (i.e. CCCS and Treasury Board of Canada Secretariat (TBS)), on Security Incident containment, eradication and recovery, in accordance with the Security Incident Response process and the GC CSEMP (https://www.canada.ca/en/government/system/digital-

government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html).

(b) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, the procedure for recovering data or the service, and records of activities related to the management of the security incident including internal communications and external communications (e.g. in the case of a ransomware event, all communications including ransom demands, etc.). This information must be provided to Canada upon request.; and

(c) Track, or enable Canada to track, disclosure of Canada's Data, including what data has been disclosed, to whom, and at what time.

(5) To support security investigations, Canada may require forensic evidence from the Contractor to assist in a GC investigation. The Contractor must:

(a) retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed or provide to Canada for retention;

(b) provide reasonable investigative support to designated, pre-authorized representatives of Canada such as CCCS and Royal Canadian Mounted Police (RCMP);

(c) maintain chain of custody for evidence in accordance with best practices such as those outlined in ISO 22095:2020;

(d) support e-discovery; and

(e) maintain legal holds to meet needs of investigations and judicial requests.

(6) In the event that the Contractor uses an external company for its incident response activities, the Contractor is expected to ensure that the provisions outlined in this *Section 28 – Security Incident Management* and *Section 29 – Security Incident Response* are also extended to the external incident response team and is documented in the Contractor's Security Incident Response Process.

29. Security Incident Response

(1) The Contractor must alert and promptly notify Canada (via phone and email), as per the reporting procedures outlined in *Section 28 – Security Incident Management)*, of any compromise, breach or of any evidence such as

(i) a security incident,

(ii) a security malfunction in any asset,

(iii) irregular or unauthorized access to any Asset,

(iv) large scale copying of an Information Asset, or

(v) another irregular activity identified by the Contractor, that leads the Contractor to reasonably believe that risk of compromise, or a security or privacy breach, is or may be imminent, or if existing safeguards have ceased to function, over the following period (7 days x 24 hours x 365 days), and will be made without undue delay, in any event, within 72 hours, and within the Contractor's service level commitments.

(2) If the Contractor becomes aware of and determines a compromise or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay

(i) notify Canada of the Security Incident;

(ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident;

(iii) take necessary steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

(iv) cooperate with Canada in investigating the occurrence, including making available all records, logs, files, data reporting, and other materials relevant to Canada's Data required to comply with applicable law or as otherwise required by Canada;

(v) identify all of Canada's Data affected or at risk of being affected;

(vi) inform Canada of the actions it is taking or will immediately take to reduce the risk of further loss to Canada;

(vii) perform or take any other actions required to comply with applicable law as a result of the occurrence;

(viii) restore any lost, corrupted or otherwise compromised data in the manner and on the schedule set by Canada without charge to Canada;

(ix) provide to Canada a detailed plan within 10 business days or as soon as reasonably practical (provided that, within 10 business days, a preliminary plan has been provided to Canada) of the occurrence describing the measures Contractor will undertake to prevent a future occurrence; and

(x) cooperate with Canada to participate in the investigation of the breach and to exercise control over reporting the unauthorized access or disclosure of Canada's Data, to the extent permitted by law and to the extent that Canada's tenant application activity audit logs are relevant to the event and investigation, and subject to the Contractor's obligations and confidentiality controls as reflected in the Contract and applicable industry certifications, including but not limited to those specified in *Section 8 (Third Party Assurance)*.

(3) The Contractor must report intended or accidental violations to data protection and cryptographic mechanisms to Canada, providing documentation and evidence on planned action or action taken to redress the situation.

(4) Contractors are to report major incidents to the police of jurisdiction when requested by Canada.

30. Information Spillage

(1) The Contractor must have a documented process that outlines its approach for an Information Spillage Incident. The process must be aligned with: (i) ITSG-33 Security Control for IR-9 Information Spillage Response; or (ii) another industry standard, approved by Canada in writing. Notwithstanding the foregoing, the Contractor's Information Spillage process must include, at a minimum:

(a) A process for identifying the specific data elements that is involved in a System's contamination;

(b) A process to isolate and eradicate a contaminated System; and

(c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

(2) Upon request of Canada, the Contractor must provide a document that describes the Contractor's Information Spillage Response Process.

31. Security Testing and Validation

(1) The Contractor must have a process to conduct a non-disruptive and non-destructive vulnerability scan or penetration test of the Cloud Services hosting Canada's data. This includes the ability to conduct regular internal and external scanning related to the GC tenancy, and when there are significant changes to the main platform, to identify any potential system vulnerabilities related to the GC tenancy by performing:

(i) vulnerability scans;

(ii) web application scans; and

(iii) penetration tests.

(2) The Contractor must develop a plan of action and milestones to document any planned remedial actions to correct weaknesses or deficiencies to the main platform in order to reduce or eliminate known vulnerabilities in the system, or those that could be related to the Cloud Services hosting Canada's data and operation of the GC tenancy.

(3) Upon request of Canada, the Contractor must provide the results of the testing of the overall platform and the plan of action and milestones documentation for planning and any review purposes.

(4) The Contractor must provide the ability to enable a self-service security health check or scoring tool that enables the measurement of the security posture of the Cloud Services configured by Canada.

32. Personnel Security Screening

(1) The Contractor must implement security measures that grant and maintain the required level of security screening for Contractor Personnel engaged in the provision of the Cloud Services and for Sub-processor personnel pursuant to their access privileges to information system assets on which Canada's Data is stored and processed.

(2) The Contractor screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

(3) Non-disclosure agreements should be in place for Contractor Personnel with access to Canada's Data.

(4) Upon request of Canada, the Contractor must provide a document that describes the Contractor's personnel security screening process. The process must provide, at a minimum:

(a) A description of the employee and Sub-processor positions that require access to Customer Data or have the ability to affect the confidentiality, integrity or availability of the Cloud Services;

(b) A description of the security screening activities and practices, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;

(c) A description of the security awareness and training as part of employment onboarding, when employee and sub-processor roles change, and on an ongoing basis, to ensure that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security;

(d) A description of the process that is enforced when an employee or sub-processor changes their role or when employment is terminated;

(e) The approach to detecting, responding, and mitigating potential insider threats and the security controls implemented to mitigate the risk of access to GC data and/or affect on the reliability of Cloud Services hosting Canada's data.

33. Physical (Data Centre / Facilities) Security

(1) The Contractor must implement physical security measures that ensure the protection of IT facilities and information system assets on which Canada's Data are stored and processed against all forms of tampering, loss, damage, and seizure.

(2) The Contractor must ensure that Data Centre Facilities that host Canada Data, use a risk-based prevent-detect-respond-recover approach, aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C). The security measures required under this include, at a minimum:

(i) Sufficient redundancy and recovery capabilities within and between the Contractor's facilities including, being geographically disparate such that the loss of one facility does not prohibit recovery of data and Canada's Data within the prescribed service level commitments;

(ii) Proper handling of IT Media;

(iii) Controlled maintenance of all information systems and their components to protect their integrity and ensure their ongoing availability;

(iv) Controlled access to information system output devices to prevent unauthorized access to Canada's Data;

(v) Limiting physical access to Canada's Data and Service Locations to authorized Cloud Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;

(vi) Escorting visitors and monitoring visitor activity;

(vii) Enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites);

(viii) Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting Canada's Data, using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms; and

(ix) Performs continuous security checks at the boundary of Service Locations and facilities for unauthorized exfiltration of information or system components.

(3) Upon request of Canada, the Contractor must provide a document that describes the Contractor's physical security measures.

(4) If any physical security measures are to change in a way that materially degrades the physical security, the Contractor must inform Canada.

34. Supply Chain Risk Management

(1) The Contractor must agree to provide information required for Canada to conduct a Supply Chain Security assessment, including information on ownership structure, corporate registration, investors and management executives, suppliers, sub-contractors, sub-processors, third-party relationships, and any other information required for such assessment.

(2) The Contractor must support the Supply Chain Security assessment by providing information on equipment, firmware, software, or any other systems as required.

(3) The Contractor must implement and maintain safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Cloud Services. This includes, but is not limited to protection throughout the systems development lifecycle

by designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain; threat awareness, education of the acquisition workforce on threats, risk and required security controls; and requiring supply chain entities to implement necessary safeguards.

(4) The Contractor must have a supply chain risk management approach including a Supply Chain Risk Management (SCRM) Plan that is aligned with one of the following best practices:

(a) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4);

(b) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or

(c) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SCRM plan.

(5) Within 90 days of contract award, the Contractor must, provide proof that the SCRM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime.

(6) The Contractor must provide Canada with a copy of the SCRM Plan on an annual basis, or upon request of Canada.

(7) In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the *Section 34 - Supply Chain Risk Management* requirements, within 90 days of contract award, the SaaS provider using a GC-approved

(i) IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

35. Sub-processors and Sub-contractors

(1) The Contractor must provide a list of Sub-processors and/or Sub-contractors that could be used to perform any part of the Work in providing Canada with the Service. The list must include the following information (i) the name of the Sub-processors and/or Sub-contractors; (ii) the identification of the Work that would be performed by the Sub-processors and/or Sub-contractors; and (iii) the location(s) where the Sub-processors and/or Sub-contractors would perform the Work.

(2) The Contractor must provide a list of Sub-processors and/or Sub-contractors within ten days of the effective date of the Contract. The Supplier must provide Canada notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Sub-processors and/or Sub-contractors at least 14-days in advance of providing those Sub-processors and/or Sub-contractors with access to Customer Data or Personal Data. The Supplier must assist Canada with verification of sub-processors within 10 working days.

(3) The Contractor must implement written policies and procedures designed to ensure the security of Information Systems and Canada's data that are to, or held by, Sub-processors and/or Sub-contractors. Such policies and procedures must address to the extent applicable:

(a) the identification and risk assessment of Sub-processors and/or Sub-contractors;

(b) minimum cyber security practices required to be met by such Sub-processors and/or Sub-contractors in order for them to do business with the Contractor;

(c) confirmation of compliance with the security obligations outlined in the Security Obligations;

(d) due diligence processes used to evaluate the adequacy of cyber security practices of such Sub-processors and/or Sub-contractors; and

(e) periodic assessment of such Sub-processors and/or Sub-contractors based on the risk they present and the continued adequacy of their cyber security practices.

36. Industrial Security Program – Security Requirement for Canadian Suppliers

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

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

(3) 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 (as required) including an IT Link at the level of PROTECTED B (as required).

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

(5) The Contractor/Offeror must comply with the provisions of the:

(a) Security Requirements Check List and security guide (if applicable), attached at Annex B and C;

(b) Contract Security Manual (Latest Edition); and

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

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.

37. Industrial Security Program – Security Requirements for Foreign Suppliers

The Canadian Designated Security Authority (Canadian DSA) for industrial security matters in Canada is the Industrial Security Sector (ISS), Public Services and Procurement Canada (PSPC), administered by International Industrial Security Directorate (IISD), PSPC. The Canadian DSA is the authority for confirming **Contractor/Subcontractor** compliance with the security requirements for foreign suppliers. The following security requirements apply to the foreign recipient **Contractor/Subcontractor** incorporated or authorized to do business in a jurisdiction other than Canada and delivering/performing outside of Canada for the Cloud Services described in the Cloud Solution, in addition to the Privacy and Security Requirements. These security requirements are in addition to those requirements identified in the Section entitled Protection and Security of Data Stored in Databases.

(1) The **Contractor/Subcontractor** certifies that the delivery and provisioning of Cloud Services under the terms of this contract must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which

Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

(2) The Foreign recipient **Contractor/Subcontractor** must at all times during the performance of the **contract/subcontract** be registered with the appropriate government administered supervisory authority in the country(ies) in which it is incorporated or operating and authorized to do business. The Foreign recipient **Contractor/Subcontractor** must provide proof of its registration with the applicable supervisory authority to the Contracting Authority and the Canadian DSA.

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

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

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

(6) The **Contractor/Subcontractor** must not grant access to **CANADA PROTECTED B** information/assets, except to personnel who have a need-to know for the performance of the **contract** and have been screened in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbssct.gc.ca/pol/doc-eng.aspx?id=28115), or use acceptable equivalent measures agreed to by Canada.

(7) **CANADA PROTECTED** information/assets, provided to the foreign recipient **Contractor/Subcontractor** or produced by the Foreign recipient **Contractor /Subcontractor**, must:

(a) not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the contract, without the prior written consent of Canada. Such consent must be sought from the Canadian DSA in collaboration with the Contracting Authority; and

(b) not be used for any purpose other than for the performance of the contract without the prior written approval Canada. This approval must be obtained by contacting the Contracting Authority (in collaboration with the Canadian DSA).

(8) The Foreign recipient **Contractor /Subcontractor** MUST NOT remove **CANADA PROTECTED** information/assets from the identified work site(s), and the foreign recipient **Contractor/ Subcontractor** must ensure that its personnel are made aware of and comply with this restriction.

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

(10) The Foreign recipient **Contractor/Subcontractor** must, at all times during the performance of the **contract** hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of **CANADA PROTECTED B**.

(11) The Foreign recipient Contractor must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that CANADA PROTECTED information/ assets pursuant to this contract has been compromised.

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

(13) Upon completion of the Work, the foreign recipient Contractor must return to the Government of Canada, all CANADA PROTECTED information/assets furnished or produced pursuant to this contract, including all CANADA PROTECTED information/assets released to and/or produced by its subcontractors.

(14) The Foreign recipient Contractor requiring access to CANADA PROTECTED information/assets or Canadian restricted sites, under this contract, must submit a

Request for Site Access to the Chief Security Officer of Name of Department/Organization of Canada.

(15) The Foreign recipient Contractor MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system and transfer via an IT link any CANADA PROTECTED B information until authorization to do so has been confirmed by the Canadian DSA.

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

(17) All Subcontracts awarded to a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

(18) All Subcontracts awarded by a third party foreign recipient are NOT to be awarded without the prior written permission of the Canadian DSA in order to confirm the security requirements to be imposed on the subcontractors.

(19) The Foreign recipient **Contractor/Subcontractor** must comply with the provisions of the Security Requirements Check List attached at Annex B and C.

(20) Despite any section of the General Conditions relating to subcontracting, the foreign recipient Contractor must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the contract unless the Contracting Authority (in collaboration with the Canadian DSA) first consents in writing.

(21) Canada has the right to reject any request made separate and apart from the authorization in this Contract in connection with the Contractor delivering Cloud Services to electronically access, process, produce, transmit or store **CANADA PROTECTED** data related to the Cloud Services in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

38. Physical Transport and Transmittal of Information

(1) The Contractor must implement measures to protect Canada's information in physical form, including assets at rest (for example, in use or in storage), in transit (for example, in transport or in transmittal), and through appropriate destruction. This includes, but is not limited to:

(a) Ensuring that portable data storage devices are properly secured at all times as appropriate to the highest level of security classification of the information stored on it, in an appropriate security container as defined by the PSPC's Contract Security Manual Chapter 6: Handling and safeguarding information and assets – Contract Security Manual - Security requirements for contracting with the Government of Canada – Security screening - National security - National Security and Defence – Canada.ca (tpsgc-pwgsc.gc.ca) and Annex C: Guidelines for safeguarding information and assets;

(b) Encrypting all Canada's information stored on portable data storage devices using a Cryptographic Module Validation Program certified encryption module, and in accordance with *Section 17 – Cryptographic Protection*, including use of Common Criteria Program accredited products;

(c) Ensuring that, prior to connecting the device to the Canada's IT network for the purpose of one-way transfers of information from the Canada's IT networks to the device, that the device is scanned for malicious software each time the device is connected to Canada's IT infrastructure

(d) Ensuring that all portable devices used to transport Canada's information must be cleared from the device to prevent information recovery, in accordance with the media sanitization requirements outlined in *Section 16 (1) - Data Disposition and Returning Records to Canada*.

(2) Protected information is considered "in transmittal" until it has reached its intended destination and has been delivered to the Contractor data center facility or opened. If opened, it must then be safeguarded, in accordance with *Section 33 – Physical Security*, and PSPC's Contract Security Manual Chapter 6: Handling and safeguarding information and assets – Contract Security Manual - Security requirements for contracting with the Government of Canada – Security screening - National security - National Security and Defence – Canada.ca (tpsgc-pwgsc.gc.ca) and Annex C: Guidelines for safeguarding information and assets;

(3) The Contractor must report any real or suspected loss or theft of portable data storage devices, in accordance with *Section 29 - Security Incident Response*, and PSPC's Contract Security Manual Chapter 6: Handling and safeguarding information and assets – Contract Security Manual - Security requirements for contracting with the Government of Canada – Security screening - National security - National Security and Defence – Canada.ca (tpsgc-pwgsc.gc.ca) and Annex C: Guidelines for safeguarding information and assets;

Appendix A – Schedule 2 - Privacy Obligations for Commercial Cloud Services (up to and including Protected B)

1. General

1.1 *Purpose*

The purpose of this Schedule is to set forth the privacy obligations of the Contractor relating to the use, collection, processing, transmission, storage or disposal of Canada's Data containing Personal Information (PI). Any Personal Information which is stored on Contractor systems or the Contractor is required to handle (collect, retain, use, disclose and dispose) must be safeguarded at all times by implementing administrative, physical and technical safeguards that are necessary to ensure the PI is protected commensurate to the level of injury that could arise if a privacy breach was to occur and in accordance with the Contractor Data Processing Agreement, this Schedule, and the Contractor's Specific Privacy Measures (collectively, the "**Privacy Obligations**").

1.2 *Flow-Down of Privacy Obligations*

The obligations of the Contractor contained in these Privacy Obligations must be flowed down by the Contractor to Sub-processors and/or Subcontractors, to the extent applicable.

1.3 *Change Management*

The Contractor must, throughout the Contract, take all steps required to update and maintain the Privacy Obligations as needed to comply with the security practices of industry standards.

The Contractor must advise Canada of all changes that materially degrades or may have an adverse effect to the Cloud Service offerings in this Contract, including technological, administrative, or other types of changes or improvements that are made, and that could impact the current collection, use, disclosure and or disposal of data containing personal information. The Contractor agrees to offer all improvements it is offering to its customers at large as part of its standard service offering at no additional cost to Canada.

2. Acknowledgments

The parties acknowledge that:

(a) All Canada's Data containing personal information are subject to these Privacy Obligations.

(b) Notwithstanding any other provision of this Schedule, the parties have shared responsibility for developing and maintaining policies, procedures and privacy controls relating to Canada's Data.

(c) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Contractor Personnel to access Canada's Data prior to the implementation of the Privacy Obligations as required under this Schedule on or before the date of Contract Award.

3. Data Ownership

(1) Canada will at all times remain the controller of the Personal Information (PI) processed by the Contractor under the Contract. Canada is responsible for compliance with Canada's privacy obligations as a controller under applicable data protection law, in particular for justification of any transmission of PI to the Contractor (including providing any required notices and obtaining any required

consents and/or authorizations, or otherwise securing an appropriate legal basis under applicable data protection law), and for Canada's decisions and actions concerning the processing of such personal data.

(2) The Contractor is and will at all times remain a processor with regard to the data containing PI provided by Canada to the Contractor under the Contract. The Contractor is responsible for compliance with its obligations under this it's Contractor Data Processing Agreement and for compliance with its obligations as a processor under applicable privacy law (i.e. Personal Information Protection and Electronic Documents Act (PIPEDA) and the *Privacy Act*).

(3) The Contractor must not use or otherwise process Canada's Data containing PI or derive information from it for any data sharing, advertising or any commercial purposes. As between the parties, Canada retains all right, title and interest in and to Customer Data. The Contractor acquires no rights in Customer Data, other than the rights Customer grants to the Contractor to provide the Cloud Services to Customer.

(4) All data that is stored, hosted or processed on behalf of Canada remains the property of Canada.

4. Privacy Requests

(1) Canada and the Contractor must establish a mutually agreeable process for dealing with requests for access to Records under the Access to Information Act and requests for access to Personal Information under the Privacy Act (Access Requests).

(2) Within 30 calendar days of Contract award, the Contractor must provide a document that describes how the Contractor will support Canada in handling Access Requests, including how it will acknowledge the receipt of an Access Request, and how it will provide the requested information.

5. Third-Party Assurance: Certifications

(1) The Contractor must ensure that in respect of any personal information including Canada's Data that it may host, store or process, on Contractor Infrastructure (including any IaaS, PaaS or SaaS Service provided to Canada) and Service Locations are secured appropriate privacy and security measures that comply with the requirements set forth the Contractor's privacy practices and policies.

(2) The Contractor must demonstrate that the measures comply with the requirements set forth in the following certifications 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 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors – Certification achieved by an accredited certification body.

(3) Each certification provided must:

(i) identify the legal business name of the Contractor or applicable Sub-processor;

(ii) identify the Contractor's or Sub-processor's certification date and the status of that certification;

(iii) identify the services included within the scope of the certification report. If the carved out method is used to exclude subservice organizations such as data centre hosting, the subservice organization's assessment report must be included.

(4) Each audit will result in the generation of an audit report which must be made available to Canada. Certifications must be accompanied by supporting evidence such as the ISO assessment report developed to validate compliance to the ISO certification and must clearly disclose any material findings by the auditor. The Contractor must promptly remediate issues raised in any audit report to the satisfaction of the auditor.

(5) The Contractor is expected to maintain its certification of ISO 27018 for the duration of the contract. The Contractor must provide, at least annually, and promptly upon the request of Canada, all reports or records that may be reasonably required to demonstrate that the Contractor's certifications are current and maintained.

6. Privacy Compliance

(1) The Contractor must demonstrate through third party assessment reports and audit reports that it:

(a) Restricts creating, collecting, receiving, managing, accessing, using, retaining, sending, disclosing and disposing of Personal Information to only that which is necessary to perform the Cloud Services; and

(b) Has implemented updated security processes and controls such as access management controls, human resource security, cryptography and physical, operational and communications security that preserve the integrity, confidentiality and accuracy of all information and data and metadata, irrespective of format.

7. Auditing Compliance

(1) In the event Canada needs to conduct security and privacy audits, inspections and/or review any additional information (e.g., documentation, data flows, data protection description, data architecture and security descriptions), both Parties agree to negotiate a solution in good faith and consider both the rationale for Canada's request and the Contractor's processes and protocols.

(2) The Contractor must conduct the privacy and security audits of the computers, computing environment and physical data centers that it uses in processing Canada's Data containing PI as follows:

(a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and

(c) Each audit will be performed by qualified, independent, third party security auditors that (i) is qualified under the AICPA, CPA Canada, or ISO certification regime,

and (ii) conforms to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

(3) Each audit will result in the generation of an audit report that must be made available to Canada. The audit report must clearly disclose any material findings by the third party auditor. The Contractor must, at its own expense, promptly remediate issues and correct deficiencies raised in any audit report to the satisfaction of the auditor.

(4) Upon request of Canada, additional supplementary evidence from the Contractor, including system security and privacy plans, designs, or architecture documents that provide a comprehensive system description including all the data elements containing PI, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) in order to demonstrate the Contractor's compliance with the required industry certifications.

8. Privacy by Design

The Contractor must demonstrate that it implements privacy by design as part of its software development lifecycle, and in accordance with Schedule 1 – Security Obligations, Section 20 (Secure by Design and Secure Development).

9. Privacy Officer

(1) The Contractor must, within 10 days of the effective date of this Contract, provide Canada with information that identifies an individual as a Privacy Officer to act as Contractor's representative for all matters related to the Personal Information and the Records. The Contractor must provide that person's name and contact information including the individual's business title, email address and phone number.

10. Assist in Delivery of Canada's Privacy Impact Assessment

(1) The Contractor must support Canada in creating a privacy impact assessment in accordance with the Treasury Board Directive on Privacy Impact Assessment (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308), by assisting Canada with the supporting documentation including a foundational PIA for Canada provided by the Contractor. The Contractor agrees to provide this support within five to ten working days of a request or within a mutually agreed upon timeframe depending on the complexity of the request by Canada.

11. Privacy Breach

(1) The Contractor must promptly evaluate and respond to incidents that create suspicion of or indicate unauthorized access to or processing of Personal Information ("**Incident**"). To the extent the Contractor becomes aware of and determines that an Incident qualifies as a breach of privacy leading to the misappropriation or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Information transmitted, stored or otherwise processed on the Contractor's systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such Personal Information ("Personal Information Breach"), the Contractor will inform Canada of such Personal Information Breach without undue delay and in accordance with Schedule 1 – Security Obligations, Section 29

(2) The Contractor must:

(a) Upon anticipation or occurrence of a privacy breach, maintain a record and notify Canada of:

i The date of the breach or the period during which it occurred and the date on which the breach was discovered;

ii A description of the breach, including its type and cause;

iii The number or approximate number of Individuals affected;

iv The personal information involved;

v A description of the relevant safeguards that were in place;

vi All remedial actions, including containment, mitigation and prevention measures, that were or will be taken;

vii The method used to notify individuals whose personal information was affected, or justification where notification will not occur.

viii The physical or geographic location where the breach occurred;

ix A list of additional parties notified of the breach; and

x The procedure for recovering the data.

(b) Tracks, or enables Canada to track, disclosures of Canada's Data, including what data has been disclosed, to whom, and at what time.

12. Personal Information

The following sub-sections applies to situations where the Contractor confirms that it has access, care, and control of Canada's data.

12.1 Ownership of Personal Information and Records

(1) To perform the Cloud Services, the foreign recipient **Contractor/Sub-processor/Subcontractor** will be provided with and/or will be collecting Personal Information from third parties. The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that it has no rights in the Personal Information or the Records and that Canada owns the Records. On request, the foreign recipient **Contractor/Sub-processor/Subcontractor** must make all the Personal Information and Records available to Canada immediately in a format acceptable to Canada.

12.2 Use of Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** agrees to create, collect, receive, manage, access, use, retain and dispose of the Personal Information and the Records only to perform the Cloud Services in accordance with the **contract**.

12.3 Collection of Personal Information

(1) If the foreign recipient **Contractor/Sub-processor/Subcontractor** must collect Personal Information from a third party to perform the Cloud Services, the foreign recipient **Contractor/Sub-processor/Subcontractor** must only collect Personal Information that is required to perform the Cloud Services. The foreign recipient **Contractor/Subprocessor/Subcontractor** must collect the Personal Information from the individual to whom it relates and the foreign recipient **Contractor/Sub-processor/Subcontractor** must inform that individual (at or before the time when it collects the Personal Information) of the following:

(a) that the Personal Information is being collected on behalf of, and will be provided to, Canada;

(b) the ways the Personal Information will be used;

(c) that the disclosure of the Personal Information is voluntary or, if there is a legal requirement to disclose the Personal Information, the basis of that legal requirement;

(d) the consequences, if any, of refusing to provide the information;

(e) that the individual has a right to request access and correct his or her own Personal Information; and

(f) that the Personal Information will form part of a personal information bank (within the meaning of the *Privacy Act*), and also provide the individual with information about which government institution controls that personal information bank, if the Contracting Authority has provided this information to the foreign recipient **Contractor/Sub-processor/Subcontractor**.

(2) The foreign recipient **Contractor/Sub-processor/Subcontractor** and their respective employees must identify themselves to the individuals from whom they are collecting Personal Information and must provide those individuals with a way to verify that they are authorized to collect the Personal Information under a Contract with Canada.

(3) If requested by the Contracting Authority, the foreign recipient **Contractor/Subprocessor/Subcontractor** must develop a request for consent or notification form to be used when collecting Personal Information, or a script for collecting the Personal Information by telephone. The foreign recipient **Contractor/Sub-processor/Subcontractor** must not begin using the form or script unless the Contracting Authority first approves it in writing. The Contractor must also obtain the Contracting Authority's approval before making any changes to a form or script.

(4) At the time it requests Personal Information from any individual, if the foreign recipient **Contractor/Sub-processor/Subcontractor** doubts that the individual has the capacity to provide consent to the disclosure and use of his or her Personal Information, the foreign recipient **Contractor/Sub-processor/Subcontractor** must ask the Contracting Security Authority for instructions.

12.4 Maintaining the Accuracy, Privacy, and Integrity of Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** must ensure that the Personal Information is as accurate, complete, and up to date as possible. The foreign recipient **Contractor/Sub-processor/Subcontractor** must protect the privacy of the Personal Information. To do so, at a minimum, the foreign recipient **Contractor/Subprocessor/Subcontractor** must:

(a) not use any personal identifiers (e.g. social insurance number) to link multiple databases containing Personal Information;

(b) segregate all Records from the foreign recipient **Contractor's/Subprocessor's/Subcontractor's** own information and records;

(c) restrict access to the Personal Information and the Records to people who require access to perform the Cloud Services (for example, by using passwords or biometric access controls);

(d) provide training to anyone to whom the foreign recipient **Contractor/Subprocessor/Subcontractor** will provide access to the Personal Information regarding the obligation to keep it confidential and use it only to perform the Cloud Services. The foreign recipient **Contractor/Sub-processor/Subcontractor** must provide this training before giving an individual access to any Personal Information and the foreign recipient **Contractor/Subprocessor/Subcontractor** must keep a record of the training and make it available to the Contracting Authority if requested;

(e) if requested by the Contracting Authority, before providing anyone with access to the Personal Information, require anyone to whom the foreign recipient **Contractor/Sub-processor/Subcontractor** provides access to the Personal Information to acknowledge in writing (in a form approved by the Contracting Authority) their responsibilities to maintain the privacy of the Personal Information;

(f) keep a record of all requests made by an individual to review his or her Personal Information, and any requests to correct errors or omissions in the Personal Information (whether those requests are made directly by an individual or by Canada on behalf of an individual);

(g) include a notation on any Record(s) that an individual has requested be corrected if the foreign recipient **Contractor/Sub-processor/Subcontractor** has decided not to make the correction for any reason. Whenever this occurs, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately advise the Contracting Authority of the details of the requested correction and the reasons for the foreign recipient **Contractor's/Sub-processsor's/Subcontractor's** decision not to make it. If directed by the Contracting Authority to make the correction, the Contractor must do so;

(h) keep a record of the date and source of the last update to each Record;

(i) maintain an audit log that electronically records all instances of and attempts to access Records stored electronically. The audit log must be in a format that can be reviewed by the foreign recipient **Contractor/Sub-processor/Subcontractor** and Canada at any time; and

(j) secure and control access to any hard copy Records.

12.5 Safeguarding Personal Information

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** must safeguard the Personal Information at all times by taking all measures reasonably necessary

to secure it and protect its confidentiality, integrity, and availability in accordance with the security measures outlined in Schedule 1 – Security Obligations.

12.6 Statutory Obligations

(1) The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that Canada is required to handle the Personal Information and the Records in accordance with the provisions of Canada's *Privacy Act*, R.S.C., 1985, c. P-21, *Access to Information Act*, R.S.C., 1985, c. A-1, and *Library and Archives of Canada Act*, S.C. 2004, c. 11. The foreign recipient **Contractor/Sub-processor/Subcontractor** agrees to comply with the requirements established by the Contracting Authority that is reasonably required to ensure that Canada meets its obligations under these acts and any other legislation in effect from time to time.

(2) The foreign recipient **Contractor/Sub-processor/Subcontractor** acknowledges that its obligations under the **contract** are in addition to any obligations it has under the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, or similar legislation in effect from time to time in any province or territory of Canada. If the foreign recipient **Contractor/Sub-processor/Subcontractor** believes that any obligations in the **contract** prevent it from meeting its obligations under any of these laws, the foreign recipient **Contractor/Sub-processor/Subcontractor** must immediately notify the Contracting Authority of the specific provision of the **contract** and the specific obligation under the law with which the foreign recipient **Contractor/Subprocessor/Subcontractor** believes it conflicts.

12.7 Legal Requirement to Disclose Personal Information

(1) If the Contractor receives any subpoena, judicial, administrative or arbitral order of an executive or administrative agency, regulatory agency, or other governmental authority which relates to the processing of Personal Information ("Disclosure Request"), it will promptly pass on such Disclosure Request to Canada without responding to it, unless otherwise required by applicable law (including to provide an acknowledgement of receipt to the authority that made the Disclosure Request).

(2) At Canada's request, the Contractor will provide Canada with reasonable information in its possession that may be responsive to the Disclosure Request and any assistance reasonably required for Canada to respond to the Disclosure Request in a timely manner.

12.8 Complaints

Canada and the foreign recipient **Contractor/Sub-processor/Subcontractor** each agree to notify the other immediately if a complaint is received under the *Access to Information Act* or the *Privacy Act* or other relevant legislation regarding the Personal Information. Each Party agrees to provide any necessary information to the other to assist in responding to the complaint and to inform the other immediately of the outcome of that complaint.

12.9 Exception

The obligations set out in these supplemental general conditions do not apply to any Personal Information that is already in the public domain, as long as it did not become part of the public domain as a result of any act or omission of the Contractor or any of its subcontractors, agents, or representatives, or any of their employees.

Annex B Statement of Challenge (SoC)

The SoC has not been modified since the initial publication of the CBS. Discussions will be held with the prequalified vendors.

IaaS Problem, Challenge Statements and Outcomes

Context

The Government of Canada (GC) has a requirement for access to Commercially Available Public Cloud Services ("Cloud Services") to meet its business needs across a broad spectrum of government organizations. In order to assist organizations in meeting Canadians' expectations and delivering government services and benefits simply, securely and efficiently, Canada is seeking the access and delivery of Commercially Available Public Cloud Services at various data classification levels.

The GC must create a secure and resilient enterprise digital security ecosystem to continue to deliver the services that Canadians rely on today while accelerating Canada's move to modern services that are secure, reliable, user-centric and barrier-free, and meeting the need for privacy and transparency[i]. This is essential to maintaining trust in Canada's institutions.

Scope

The scope of the resulting contract is to resolve the problem, address the challenges and produce the expected outcomes. The scope will remain stable during the contract's life but the way the cloud services will be rendered may evolve.

Problem Statement and Challenges

Problem Statement

Canada lacks the ability to deploy digital infrastructure with agility and velocity, as well as capacity to scale and leverage emerging technologies to advance its service delivery for Canadians.

Challenges

Canada's application environment is characterized by an aging, legacy infrastructure limiting its ability to advance its digital agenda. Couple that with a large sensitive data set, which, if compromised, would have a significant impact on the security and privacy of Canadians, the GC and stakeholders.

The following challenges limit Canada's capacity to resolve the problem:

a. The complexity related to a high dependency on legacy systems and an aging infrastructure.
b. The difficulty with addressing demand fluctuations and to scale on-premises services in a timely manner.
c. The complexity of integrating and connecting Cloud services with on-premises services.
d. The application of the GC's stringent security and privacy standards, as well as government policies and regulations.

e. The limited capacity to forecast and manage the cost of Cloud services due to the lack of enterprise-level visibility on detailed service costs and consumption.
f. The recruitment, retention, and training of skilled professionals necessary to implement ever-evolving Cloud services.

Expected Outcomes of the Contract

The GC must continue to address the challenges of digital modernization and the risks of its aging IT systems to provide long-term benefits to all the people and businesses it serves, including GC employees. The ability of the Government to deliver both large technical modernization and iterative improvements is critical to improve what Canadians experience in the digital age.

For the initial increment, Canada expects to procure technologies based on highly scalable cloud platform solutions that facilitate faster idea-to-value transformation, robust security, and compliance mechanisms, along with financial predictability.

The GC must continue to provide a secure, reliable, and privacy-enabled, interoperable service delivery environment for internal services and business applications that are hosted in cloud-based environments. This will enable continuous improvement of Canada's digital service delivery to meet its evolving needs, ambition, and commitments.

[i] Digital Ambition - Canada.ca

MVR IaaS – Native PaaS Procurement

WORKING DRAFT

The MVRs will be subject to discussion with prequalified vendors.

Minimum Viable Requirements (MVRs)

The sections below describe the expected minimal capabilities of the Solution. It describes what the Solution must be able to do (functional requirements), and how the Solution must interact with the environment and other devices (non-functional requirements). The MVRs are mandatory.

1. **General**

   1.1 The bidder must offer services that are Commercially Available with publicly accessible documentation. These services must also come with comprehensive support, including technical assistance, defined service level agreements (SLAs), and regular updates.

2. **Compute**

   2.1. The solution must include compute instances to provide computing resources for running applications and workloads in the cloud.

3. **Storage**

   3.1. The solution must include Block, Object and File storage capabilities that are scalable.

4. **Operational and Security Dashboards, Reporting and Logs**

   4.1. The solution must include a centralized dashboard to access information and metrics to monitor and report on the infrastructure and workloads including health status, security posture, and compliance dashboard.

5. **Centralized Automated Configurations**

   5.1. The solution must be configurable and consumable through Infrastructure as Code (IaC) either through a native automation system or a third-party solution.

   5.2. The solution must be able to integrate with services and systems using an Application Programming Interface (API) system.

6. **Resiliency Requirements**

   6.1. Must have a minimum of two geographically redundant regions and two data centres per region to allow for seamless failover from one to the other with no material impact on operations nor shall it require operational input from the GC to manage.

   6.2. The solution must include redundancy and failover mechanisms at various IaaS and PaaS levels, including compute, storage, and networking, to mitigate single points of failure.

7. **Scalability**

   7.1. The solution must be able to scale resources horizontally and vertically to accommodate increased demand without service degradation, including auto-scaling policies, elastic load balancing, and capacity planning.

8. **Network Capacity**

   8.1. Network capacity refers to the amount of network resources and bandwidth available within the IaaS environment which determines how much data can be transferred between virtual machines (VMs), storage resources, and other components within the infrastructure.

   8.2. The solution network must connect to the Secure Cloud to Ground requirements of the GC.

9. **Native and 3rd Party Firewall Capabilities**

   9.1. The solution must include a native firewall capability that is configurable to manage security groups.

9.2. The solution must be able to use 3rd party firewalls and security appliances (e.g., Fortinet and F5).

9.3. The solution must include a Web Application Firewall (WAF) to protect web applications from various online threats and attacks.

9.4. The solution must include an Intrusion Detection System (IDS) as a security mechanism that monitors network or system activities for signs of unauthorized access, security policy violations, and suspicious behaviour.

10. Tagging/Identification of Assets

10.1. The solution must have a tagging mechanism for all assets and services.

11. Multi-Factor Authentication (MFA) administrative access control

11.1. The solution must secure both portal and API access using multi-factor authentication (MFA) through its native Identity and Access Management (IAM) system.

12. Threat monitoring and Vulnerability assessment

12.1. The solution must provide a threat detection service that continuously monitors for potential threats.

12.2. The solution must have a service that assesses compute instances for security vulnerabilities and threats.

13. Connectivity

13.1. The solution must enable Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to secure data transmission.

13.2. The solution must provide a secured REST API for application integration and data exchange for sources internal and external to the solution.

14. Financial Controls

14.1. The solution must include financial controls for overall expenditure, and mechanisms to prevent specific elements from being used without permission given by SSC’s delegating authority.

Annex E Defined Terms

Term	Definition
Agent	An agent authorized by the Contractor that can perform one or more of the following duties under the terms of the TAC and any corresponding TA: 1) provide billing information 2) invoicing 3) provide consumption reporting services 4) receive payment on behalf of the Contractor An agent does not have or provide SSC access to any master accounts, nor do they have access to a client tenant, client data or client master accounts.
Canada's Data	Information or data, including all text, sound, video, or image files, software and related metadata, regardless of form or format: (A) disclosed by Canada's personnel, clients, partners, joint venture participants, licensors, vendors or suppliers through the use of the Cloud Services. (B) disclosed by End Users of the Cloud Services; or (C) collected, used, processed by, or stored within the Cloud Services, which is directly or indirectly disclosed to the Contractor or Subcontractors by or on behalf of Canada or through the use of the Cloud Services including any such information or data to which (i) the Contractor or any Subcontractors obtain access, intentionally or inadvertently. (ii) resident on any network, System or Hardware used or managed for Canada by the Contractor for the Cloud Services and Contractor's services, including Contractor Infrastructure.
Cloud Computing	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,

	networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Definition taken from the Institute of Standards and Technology (NIST) definition of Cloud Computing, located in SP 800-145 at the following link: http://csrc.nist.gov/publications/PubsSPs.html#800-145
Cloud Services(s)	Cloud Services are service offerings which deliver a Cloud computing model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud Service Provider (CSP)	A Cloud Service Provider is an entity (can include one or more natural persons, corporations, partnerships, limited liability partnerships, etc.) that is the originator of the Public Cloud Service in its entirety.
Commercially Available	A service available to the public to obtain for use or consumption.
Compromise	A breach of government security which includes, but is not limited to: • unauthorized access to, disclosure, modification, use, interruption, removal, or destruction of sensitive information or assets, causing a loss of confidentiality, integrity, availability or value. • any action, conduct, threat or gesture of a person toward an employee in the workplace or an individual within federal facilities that caused harm or injury to that employee or individual; and, • events causing a loss of integrity or availability of government services or activities. (Reference: GC Cyber Security Event Management Plan)
Contractor	A Contractor is the entity (can include one or more natural persons, corporations, partnerships, limited liability partnerships, etc.) delivering the Cloud Services to the Government of Canada and its partners. It is the entity approved referenced as the 'Contractor' on the Resulting Contract.
End User	Any individual, or system process acting on behalf of an individual, authorized by Canada to access the Cloud Services.

Information Assets	Any individual data element of such Canada Data.
Information Spillage	Refers to incidents where an Information Asset is inadvertently placed on an Asset or System that is not authorized to process it (e.g., ITSG-33, IR-9).
Infrastructure as a Service (IaaS)	The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, including operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).
Managed Service Provider	A supplier to the Government of Canada who offers business or technology services for GC programs and service. MSPs are often viewed as outsourcing a line of business under accountability of the GC. MSPs often take on the responsibility of delivering a line of business or a portion of technology delivery. The contractual relationship between the GC and an MSP is typically governed by a Service Level Agreement (SLA). An MSP may use one or more Cloud Service Providers to deliver the technology components of their services such as self-service portals, case management, and analytics. The GC does not hold a direct contractual relationship with the CSP, but instead the GC holds the MSP contractually accountable for the CSP's services. The GC is a consumer of the MSP's services and in-turn the MSP is a consumer of the CSP's services. Alternate definition - Cyber security considerations for consumers of managed services (ITSM.50.030) - Canadian Centre for Cyber Security – Section 1.1
Master Account	An account with root level privileges to generate client accounts or sub-accounts that will enable departmental access to commercially available public cloud services.
Metadata	Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data formats, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels). (Reference: NIST SP 800-53 Rev. 4)

Native PaaS	Native PaaS is defined as PaaS supported, managed and operated by the Bidder (first-party PaaS of the CSP).
Personal Information	Information that is about an identifiable individual and recorded in any form, as defined in section 3 of the Privacy Act. Examples include but are not limited to the information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual. (Reference: https://laws-lois.justice.gc.ca/eng/acts/P-21/section-3.html)
Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer created or acquired applications created using programming languages, libraries, services and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but controls deployed applications and possibly configuration settings for the application-hosting environment.
PaaS Infrastructure	Platform infrastructure managed by the Contractor and provided as a Service (e.g., Data Centre, Networking, Storage, Servers, Virtualization platform, O/S, Middleware, and Runtime), including the Systems, Hardware and Software used to manage, operate, and provision the PaaS Infrastructure.
Privacy Breach	A privacy breach involves the improper or unauthorized collection, use, disclosure, retention and disposal of Personal Information.
Processor	Means a natural or legal person, public authority, agency or other body that processes Personal Information on behalf of, and in accordance with the instructions of, Canada.
Public Cloud Services	“Public Cloud” means the cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider. Public Cloud Services refers to a shared pool of configurable Cloud Computing service models made available to users as a rapid, on demand, elastic self-service

	via the Internet from a Cloud Service Provider's servers as opposed to being provided from a company's own on-premise servers.
Record	Any hard copy document or any data in a machine-readable format containing Personal Information
Security Event	An event, omission or situation may be detrimental to government security, including threats, vulnerabilities, and security incidents. Examples of cyber security events include but are not limited to disclosure of new vulnerabilities, intelligence that a threat actor may be planning an attack against a GC information system - e.g., Distributed Denial of Services (DDOS) attack; and attempts at breaching the network perimeter, etc.
Security Event Log	Any event, notification or alert that a device, systems or software is technically capable of producing in relation to its status, functions and activities. Security Events Logs are not limited to security devices, but are applicable to all devices, systems and software that are technically capable of producing event logs that can be used in security investigations, auditing and monitoring. Examples of Systems that can produce security event logs are, but not limited to: firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, DHCP, DNS, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, applications/layer 7 firewalls.
Security Incident	Any event (or collection of events), act, omissions or situation that has resulted in a compromise. Examples of cyber security incidents: Active exploitation of one or more identified vulnerabilities, exfiltration of data, failure of a security control, breach of a cloud-hosted or managed GC service, etc. (Reference: GC Cyber Security Event Management Plan)
Services	a) Granting usage rights to the Cloud Service(s); providing Cloud Service(s) Documentation. b) maintaining, upgrading and updating the Cloud Service(s). c) managing incidents and defects to ensure the Cloud Service(s) operates at the applicable service levels; and

	d) providing incidental and additionally required information technology infrastructure services required to deliver the Cloud Service(s).
Security Event	Any event, omission or situation that may be detrimental to government security, including threats, vulnerabilities and security incidents. Examples of cyber security events: Disclosure of a new vulnerability, intelligence that a threat actor may be planning an attack against a GC information system (e.g., Distributed Denial of Service (DDOS) attack), attempts at breaching the network perimeter, etc. (Reference: GC Cyber Security Event Management Plan)
Service Level Agreement (SLA)	Service Level Agreement is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider.
Service Location(s)	Any facility, site or other physical location owned, leased, provisioned or otherwise occupied by the Supplier or any Supplier Sub-processor from which the Supplier or any Supplier Sub-processor provides any Services.
Software as a Service (SaaS)	SaaS pertains to the service model through which the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (e.g., web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Subcontractor	Any person to whom the Contractor subcontracts the performance of the Contractor's services, in whole or in part.
Sub-processor	Any a natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller or Contractor.

System	Any combination of hardware and software, including any communications line or network device, used to provide the link between this combination of hardware and software related to the services.
User	A User is any individual or system process acting on behalf of an individual authorized by Canada to access the Services.

Attachment 1 – Prequalification Evaluation Grid

Part A – Mandatory Criteria

The following mandatory criteria must be met.

	Criteria	Information required by Bidders	Scoring Elements
M1	**Capacity of the Bidder to sell Commercially Available Infrastructure-as-a-Service (IaaS) AND Platform-as-a-Service (PaaS)** The Bidder must be a Cloud Service Provider (CSP) with Commercially Available Infrastructure-as-a-Service (IaaS) services **AND** Native Platform-as-a-Service (PaaS) services.	The Bidder should provide the hyperlink publicly available listing the Commercially Available IaaS and Native PaaS services of the following: 1. services (instance types) that address each category of the following Commercially Available IaaS services: a. Category 1 - General or Standard Purpose instances that are configurable to balance the amount of compute, memory, and networking resources based on the requirements of applications and workloads. b. Category 2 - Compute Optimized instances for applications and workloads that require high computing power using high-performance processors. c. Category 3 - Memory Optimized instances for applications and workloads that require fast processing of large data sets in memory. d. Category 4 - Specialized instances for applications and workloads that require specific requirements, including any of the following sub-categories: i. High-Performance Computing (HPC) ii. Enhanced storage capabilities iii. GPU-supported processes iv. Machine learning-based systems e. Category 5 - Block, Object and File storage capabilities that are scalable. f. Category 6 - Cold storage for long-term storage of archived data. g. Category 7 - High-Performance storage based on Solid-State Drives (SSD) technology. 2. services (instances type) that address each category of the following Native PaaS services: a. Category 8 - Container services b. Category 9 - Developer tools c. Category 10- Database services	To be compliant, the bidder must demonstrate the following services through hyperlinks: • A minimum of 5 Commercially Available IaaS services for each of the category evidenced by their publicly viewable product/service list (1a to 1g) • A minimum of 4 Commercially Available PaaS services for each of the category evidenced by their publicly viewable product/service list (2a to 2f) *Note: If a broken hyperlink is provided in the Prequalification Bidding Form, SSC reserves the right to request clarification from the bidder; however, the services specified must remain consistent with the original proposal.*

	Criteria	Information required by Bidders	Scoring Elements
		d. Category 11 - Network and security services e. Category 12 - Artificial Intelligence (AI) or Machine Learning (ML) f. Category 13 - Analytics and Big Data services	
M2	**Capacity of the Bidder to secure Canada's Data** The Bidder must have the following current, latest version and valid industry certifications and audit reports: 1. ISO/IEC 27001: Information technology – Security techniques - Information security management systems – Requirements; 2. ISO/IEC 27017: Information technology – Security techniques - Code of practice for information security controls based on ISO/IEC 27002: for cloud services; 3. AICPA Service Organization Control (SOC) 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality. *Only certifications issued by an independent third party qualified under AICPA, CPA Canada, or conforming to the ISO/IEC 17020 quality system standard will be accepted.	The Bidder should provide the following evidence for each certification and audit reports: - copies of the certifications and audit reports. - a verification letter or statement from the issuing body confirming the current and valid status of the certification. - the date of issuance and expiration.	To be compliant, the Bidder must demonstrate they have current, latest version and valid certifications and audit reports of the following: ISO/IEC 27001, ISO/IEC 27017 and AICPA Service Organization Control (SOC) 2 Type II.

Part B – Rated Criteria

The following criteria will be rated as per the scoring elements defined in the table.

Maximum total score = 77 points

	Criteria	Information to be provided by Bidders	Scoring Elements
R1	**Capacity to satisfy data residency requirements (maximum 15 points)** The Bidder should have a minimum of one data centre located in Canada. Canada uses the Uptime Institute's Tiered Classification System for the Data Centre definition. For the purpose of this solicitation, a Data Centre is a physical infrastructure that meets or exceeds the "Data Center Tier III" requirements.	The Bidder should provide the physical address of one data centre located in Canada.	Up to 15 points will be allocated. Points will be allocated as follows: • the bidder has a data center located in Canada = 15 points • the bidder has not a data center located in Canada = 0 points.
R2	**Capacity of the Bidder's Solution to protect Canada's data (maximum 12 points)** The Bidder should demonstrate that the Solution has the capability to encrypt data-in-transit and data-at-rest with Communications Security Establishment Canada (CSE) approved cryptography. *Note to Bidders: This requirement is not mandatory for the prequalification stage. It will be mandatory in subsequent procurement stages and will be verified prior to contract award.* The CSE approved cryptography can be found in the Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information - ITSP.40.111 (version 3 – March 18, 2024) (https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111)	**1. For Data-in-transit:** To demonstrate its capacity, the Bidder should provide the cryptographic mechanism used to prevent unauthorized disclosure of information and detect changes to information during transmission, and provide evidence for the following elements: a) Identify if Cryptographic modules have been tested and validated under the Cryptographic Module Validation Program (CMVP) for compliance to FIPS 140-3: Security Requirements for Cryptographic Modules as per Section 12 of ITSP 40.111 b) Identify which encryption algorithms are implemented, and confirm that they are part of the suite of recommended encryption algorithms as per Sections 2 and 3 of ITSP 40.111 c) Confirm whether Cryptographic algorithm implementations have been tested and validated under the Cryptographic Algorithm Validation Program (CAVP) as per Section 12 of ITSP 40.111.	Up to 12 points will be allocated. Points will be allocated as follows: **1. For Data-in-transit:** a) FIPS 140-3 CMVP validated = 2 points Previous FIPS version CMVP validated = 1 point Not CMVP validated = 0 points b) Encryption algorithm is on list of CSE recommended = 2 points Encryption algorithm is on list of CSE sufficient = 1 point Any other algorithm = 0 points c) Validated under the CAVP = 2 points Not validated under the CAVP = 0 points **2. For Data-at-rest:**

	Criteria	Information to be provided by Bidders	Scoring Elements
		2. For Data-at-rest: To demonstrate its capacity, the Bidder should provide the cryptographic mechanism used to prevent unauthorized disclosure and modification of the information at rest on information system components storing Canada's data and provide evidence for the following elements: a) Identify if Cryptographic modules have been tested and validated under the Cryptographic Module Validation Program (CMVP) for compliance to FIPS 140-3: Security Requirements for Cryptographic Modules as per Section 12 of ITSP 40.111 b) Identify which encryption algorithms are implemented, and confirm that they are part of the suite of recommended encryption algorithms as per Sections 2 and 3 of ITSP 40.111 c) Confirm whether Cryptographic algorithm implementations have been tested and validated under the Cryptographic Algorithm Validation Program (CAVP) as per Section 12 of ITSP 40.111. For each element, the following evidence could be provided: 1. system and communications protection policy; 2. procedures addressing protection of information at rest and in-transit; 3. information system design documentation; 4. information system configuration settings and associated documentation; 5. cryptographic mechanisms and associated configuration documentation; 6. information system audit records; 7. other relevant documents or records	Points will be allocated as follows: a) FIPS 140-3 CMVP validated = 2 points Previous FIPS version CMVP validated = 1 point Not CMVP validated = 0 points b) Encryption algorithm is on list of CSE recommended = 2 points Encryption algorithm is on list of CSE sufficient = 1 point Any other algorithm = 0 points c) Validated under the CAVP = 2 points Not validated under the CAVP = 0 points
R3	**Experience of the Bidder to provide IaaS and Native PaaS services to large organizations (maximum 21 points)** The Bidder should demonstrate its experience in providing both IaaS and Native PaaS services to large	To demonstrate its experience, the Bidder should provide a list of three clients to whom both IaaS and Native PaaS services were provided.	Up to 21 points will be allocated using the average of the three clients' total points. Points will be allocated as follows: **Duration of services rendered to the client**

	Criteria	Information to be provided by Bidders	Scoring Elements
	government organizations or large external private corporations. *"external" refers to organizations or corporations that are not part of the bidder's own corporate structure or its parent organization.* *In this criterion "unique services" means a specific element of the commercially and publicly available cloud services catalogue. This specifically excludes non-public cloud services including but not limited to private cloud services and data center hosting services.*	For each client, the following information should be provided: 1) Client business name 2) Duration of services including service start date and end date (if applicable) (month and year) 3) Number of employees of the client 4) Number of unique services provided and used by the client within the duration of services.	- more than or equal to 7 years = 7 points - more than or equal to 5 years and less than 7 years = 5 points - more than or equal to 3 years and less than 5 years = 3 points - less than 3 years: 0 points **Number of employees of the client** - 50,000 employees and more = 7 points - between 29,999 and 50,000 employees = 5 points - between 9,999 and 30,000 employees = 3 points - fewer than 10,000 employees = 0 points **Unique services provided and used** - 200 services and more = 7 points - between 149 and 200 services = 5 points - between 99 and 150 services = 3 points - fewer than 100 services = 0 points If more than three clients are submitted, only the first three clients listed in the submission will be assessed.
R4	**Capacity of the Bidder to resolve the problem statement (maximum of 29 points)** The Bidder should demonstrate its capacity to resolve the problem in the Statement of challenges *Region is defined as multiple data centres located within 100 km of each other within the same defined region.*	The Bidder should provide the following information to demonstrate its capacity to solve the problem identified in the Statement of Challenges for each element listed below: **Elements of comparison** 1. Number of Regions in Canada. 2. Number of Regions in the World. 3. Number of Data Centres (DC) in Canada. The bidder should provide the city of each DC associated with the region. 4. Total number of Data Centres deployed and in service in the World. 5. Number of network connections in Canada. The bidder should provide the name of the	Up to 29 points will be allocated using the sum of the comparative assessment and direct scoring of the elements (1 to 11). Each element (1 to 11) will individually be assigned points. **Comparative assessment of elements** For elements 1 to 9: A. **Establishing the ranking**: Bidder will be ranked from the highest number to the lowest number. B. **Allocating the points:** points will be allocated based on the Bidder's ranking in each element, from highest to the lowest.

	Criteria	Information to be provided by Bidders	Scoring Elements
		corporations of each network connections they are with. 6. Number of network peering points globally. 7. Bandwidth capacity in gigabits per second in Canada. The bidder should provide the gigabits per second. 8. Total number of cores deployed in Canada. 9. Percentage of available capacity in terms of cores. The bidder should provide the data associated with the following calculation: The percentage of available capacity in terms of cores is calculated by [1-(number of cores in use in Canada/by number of cores deployed in Canada (item 8))]*100. **Direct scoring** 10. The bidder has documentation that defines latency and performance metrics between their Canadian regions: yes or no 11. The bidder offers a Marketplace for 3rd party apps: yes or no For elements 10 and 11: The bidder should provide the hyperlinks.	Points will be allocated for each element of comparison as follows: - Top rank bidder = 3 points - Second rank bidder = 2 points - Third rank bidder = 1 point - Remaining ranked bidder (4+) = 0 points **Direct scoring of the elements** For elements 10 and 11, points will be allocated as follows: - Yes = 1 point - No = 0 points

Attachment 2 - Rules of Engagement

Canada will engage Bidders regularly over the upcoming months in the development of the solicitation.

By participating to the consultation process, the Bidder:

1. Acknowledges and agrees that:

- The Bidder will actively participate in interactive events with Canada (interactive group sessions, one-on-one sessions, surveys) throughout the consultation process;
- A initial group session will take place during which Canada will present to the Bidder the challenges Canada is facing and for which it requires a solution;
- During the interactive events, Bidder will propose to Canada innovative approaches to meet these challenges;
- Bidder will participate and share ideas willingly and these events will not be subject to any non-disclosure agreement;
- Bidder will have equal opportunity to share preliminary ideas, which Canada could potentially use to develop the solicitation; and
- Every event will be recorded for documentation purposes to demonstrate, if required, that the consultation process was conducted fairly by Canada.

2. Undertakes to:

- Work within defined parameters that will be provided at the beginning of the consultation process, such as timelines;
- Foster fairness and transparency during the consultation process through open communication and information sharing with Canada;
- Raise any fairness or transparency concerns about this process with the Contracting Authority in a timely manner; and
- Participate in this process in an open, honest and respectful manner.