SHARED SERVICES CANADA

CBSOS - Initial

For

CLOUD SECURITY SERVICES (CCS)

Solicitation No.	CSS092421A	Date	Friday, September 24th, 2021.

GCDocs File No.	101691102

Issuing Office	Shared Services Canada 180 Kent Street, 13th Floor Ottawa, Ontario K1P 0B5	
Standing Offer Authority (The Standing Offer Authority is the person designated by that title in the Solicitation, or by notice to the Offeror, to act as Canada's "Point of Contact" for all aspects of the Solicitation process.)	Title	Christopher Bromfield
	Telephone No.	(343) 550-3959
	Email Address	christopher.bromfield@canada.ca
Closing Date and Time Solicitation Closing	Friday, January 28th, 2022 at 15:00	
Email Address for Submitting Offers	christopher.bromfield@canada.ca	
Time Zone	EST	
Destination of Goods/Services	See Herein	
Vendor/Firm Name and Address	Telephone No. :	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)	Name/Title Signature Date	

Table of Contents

SECTION 1 - GENERAL INFORMATION 4

1.1 Structure of the Challenge-Based Standing Offer Solicitation (CBSOS) 4
1.2 Problem Statement 4
1.3 CBSOS Process 5
1.4 CBSOS Stages - Infographic 6
1.5 Work Segments (WS) - Standing Offer Call-ups 8
1.6 Choice of Solutions 9
1.7 Financial Capability Assessment 10
1.8 Security Requirements 10
1.9 Cloud Security Requirements 10

SECTION 2 - OFFEROR'S INSTRUCTIONS 11

2.1 Standard Instructions, Clauses and Conditions 11
2.2 Standard Instructions 11
2.3 Consideration of Additional Terms 12
2.4 Enquiries - Solicitation 13
2.5 Point of Contact (PoC) 13
2.6 Offeror's Bilingual Information Webinar 14
2.7 Invitation to Refine 14
2.8 Window of Opportunity for Underrepresented Groups (URG) including Small and Medium Enterprises (SMEs) 16
2.9 Applicable Laws 16
2.10 Trade Agreements 16
2.11 Certifications Precedent to Standing Offer Award and Additional Information 17

SECTION 3 - OFFER PREPARATION INSTRUCTIONS 18

SECTION 4 – EVALUATION PROCEDURES AND BASIS OF SELECTION 19

SECTION 5 STANDING OFFER 20

5.1 Offer 20
5.2 Series of Standing Offers 20
5.3 Standing Offer Award and Work Segment 1 Call-ups - Proof of Concept 21
5.4 Work Segments - Standing Offer Call-ups 21
5.5 Call-up Instrument and Procedures 23
5.6 Standing Offer Call-up Allocation Method (CAM) 24
5.7 Standing Offer Reporting - Standing Offer Holders 24
5.8 Challenge-Based Standing Offer Holders List - Refresh 25
5.9 Suspension or Set Aside of Standing Offer by Canada 25
5.10 Standing Offers Reporting - Standing Offer Users 26
5.11 Standard Clauses and Conditions 26
512 Security Requirements 26
5.13 Cloud Security Requirements 26
5.14 On-going Supply Chain Integrity (SCI) Process 27
5.15 Evolving Cyber Security Requirements (Evergreen) 27
5.16 Data Ownership and Sovereignty 27
5.17 Term of Standing Offer 27

5.18 AUTHORITIES 28
5.18.4 JOINT VENTURE 28
5.19 IDENTIFIED USERS 29
5.20 PRICE ADJUSTMENT MECHANISM 29
5.21 EXCHANGE RATE FLUCTUATION 30
5.22 FINANCIAL LIMITATION TOTAL 30
5.23 DIRECT REQUEST BY CUSTOMER DEPARTMENT 30
5.24 TAXES - FOREIGN-BASED CONTRACTOR 30
5.25 CERTIFICATIONS OF COMPLIANCE 30
5.26 APPLICABLE LAWS 31
5.27 FOREIGN NATIONALS 31
5.28 INSURANCE – NO SPECIFIC REQUIREMENT 31
5.29 LIMITATION OF LIABILITY - PUBLIC CLOUD SOFTWARE AS A SERVICE (SAAS) 31
5.30 SAFEGUARDING ELECTRONIC MEDIA 32
5.31 PRIORITY OF DOCUMENTS 32

SECTION 6 RESULTING CONTRACT CLAUSES 32

6.1 STATEMENT OF CHALLENGE 33
6.2 STANDARD CLAUSES AND CONDITIONS 33
6.3 TERM OF CONTRACT 34
6.4 PAYMENT 35
6.5 INVOICING INSTRUCTIONS 38
6.6 LIMITATION OF EXPENDITURE 39

ATTACHMENT A - STATEMENT OF CHALLENGE 41

PROBLEM STATEMENT, CHALLENGES, MINIMUM VIABLE REQUIREMENTS AND PERSONAS 41

ATTACHMENT A1 - CLOUD SECURITY REQUIREMENTS 55

CLOUD SECURITY REQUIREMENTS 55

Shared Services Canada
Challenge-Based Standing Offer Solicitation

Canada, as represented by the Minister of Digital Government, hereby requests a Standing Offer(s) on behalf of the Identified Users herein.

Shared Services Canada (SSC), Centre of Expertise in Agile and Innovative Procurement (CoEAIP) is currently piloting a renewed contracting framework: Agile Procurement Process 3.0 (APP3.0). APP3.0 proposes tools and flexible contracting mechanisms to improve the ability of Canada to move quicker and produce better results leveraging the procurement function. This Challenge-Based Standing Offer Solicitation is one of CoEAIP's pilots.

SECTION 1 - GENERAL INFORMATION

1.1 Structure of the Challenge-Based Standing Offer Solicitation (CBSOS)

The CBSOS is divided into six Sections plus Annexes and Attachments.

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

Section 2 Instructions to Offerors: provides the instructions, clauses, and conditions applicable to the CBSOS.

Section 3 Offer Preparation Instructions: provides Offerors with instructions on how to prepare their Offers.

Section 4 Evaluation Procedures and Basis of Selection: describes how the evaluation will be conducted, and the evaluation criteria that will be used, and the basis of selection for Challenge-Based Standing Offer award.

Section 5 Standing Offer: includes the Challenge-Based Standing Offer and the applicable terms and conditions.

Section 6 Resulting Contract Clauses: includes the clauses and conditions which will apply to any Contract resulting from a Call-up made pursuant to the Standing Offer.

Annex and Attachments

Annexes and Attachments: includes the Annexes, supplemental material to the CBSOS and Attachments, supplemental material to the Standing Offer and Resulting Contract Clauses.

1.2 Problem Statement

Canada lacks an enterprise cloud-based security solution that provides the ability to deliver a consistent user experience from any device, any location, at any time.

In certain cases, Canada lacks cost-effective consistent security controls to protect Government of Canada (GC) data and assets to GC department remote sites and GC and Non-GC remote users, including SDAs (small department and agencies), when accessing the Internet, cloud-based SaaS, LaaS, and PaaS, and GC on-premise services. This results in lost productivity, high cost, lower user satisfaction and morale, increased cybersecurity risks, and inconsistent user experience.

In order to solve the problem(s) Canada wishes to improve and optimize the ability to securely consume and deliver cloud-based services effectively, efficiently, and quickly.

Refer to Attachment A - Statement of Challenge for a detailed description of the preliminary Statement of Challenge elements, including the Problem Statement, Challenges, Minimum Viable Requirements and Personas.

(Note to Offerors: The scope of the Standing Offer may evolve as innovative components become available, which could help solve the problem(s).

1.3 CBSOS Process

Unlike traditional procurement, CBSOSs are based on the concept that Canada can best perform procurement if it presents the requirement as a need (problem statement(s)) and allows industry the freedom to propose innovative Solutions that fill the need. CBSOSs are issued in terms of needs and are accompanied by contractual conditions outlining industry participation, including mechanisms for evaluating proposed Solutions. Solutions typically take the form of "Proof of Concepts", and evaluations assess how well Solutions satisfy the need.

The CBSOS process is divided into two Components: **Invitation to Refine (ItR) - Waves 1** and **Final CBSOS**.

1.3.1 ItR - Wave 1 (Part A) - Discussion with the Software Publisher (SP)/Original Equipment Manufacturer (OEM)

Canada plans to implement an efficient and effective ItR process; throughout the ItR Wave 1 - Part A, up to 10 SP/OEM Offerors, offering a "distinct solution", will be invited to provide feedback on the problem statement(s) by participating in videoconference interactions (ItR events), answering surveys, and other types of activities facilitated by Canada, in order to help Canada, characterize what industry has to offer, and to finalize the CBSOS.

1.3.1.1 Software Publisher and Original Equipment Manufacturer - Defined

For the purpose of this Solicitation, the following definitions apply.

Software Publisher: An organization that develops and markets software. It includes market research, software production and software distribution. Publishers may develop their own programs, or contract for outside development. The titles "software publisher," "software developer" and "developer" are used synonymously; however, "developers" may be limited to designing the user interface and programming, whereas a "publisher" implies distribution and marketing as well as development.

Original Equipment Manufacturer: The company that makes the products (the "original" manufacturer).

1.3.1.2 Distinct Solutions

Solutions that are "distinct" from one another means Solutions that are comprised of:

- dissimilar *software* (as defined in 01*, Interpretation of the Supplemental General Conditions – Contractor to Own Intellectual Property Rights in Foreground Information*);
- *dissimilar Intellectual Property* (as defined in 01, *Interpretation of the Supplemental General Conditions – Contractor to Own Intellectual Property Rights in Foreground Information*; and

- *dissimilar codebases* i.e., a codebase (or code base) is a collection of source code used to build a particular software system, application, or software component.

(Note to SP/OEM Offerors: SP/OEM Offerors who have not participated in ItR Wave 1 - Part A, will be given an opportunity to provide feedback at a later date in the Solicitation process, and will be eligible to submit Offers.)

1.3.2 ItR - Wave 1 (Part B) - Discussion with Resellers of SP/OEM Solutions

Canada plans to implement an efficient and effective ItR process; throughout the ItR Wave 1 - Part B, Canada will interact in online forums with SP/OEM Solution Resellers who will be invited to provide feedback, in order to help Canada, determine the best way to leverage Resellers at the Contract stage, and to help Canada finalize the CBSOS.

1.3.2.1 Reseller – Defined

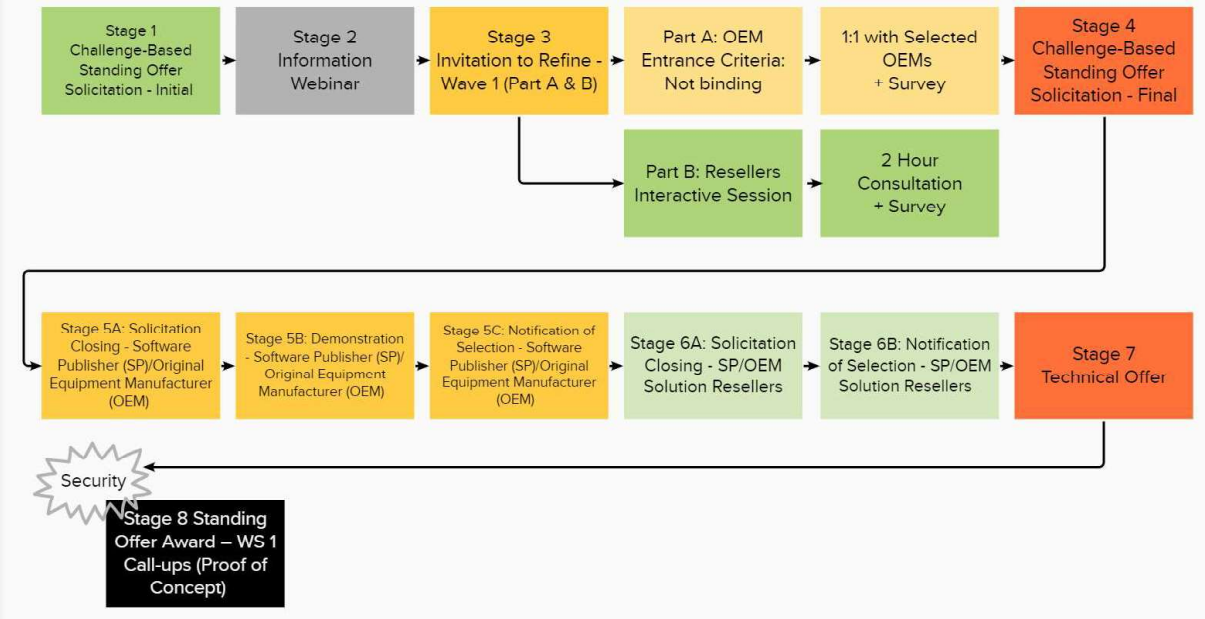
For the purpose of this Solicitation, the following definition applies.

Reseller: An organization that sells hardware and software to the general public. Resellers purchase products from software publishers and hardware manufacturers.

(Note to SP/OEM Solution Resellers: SP/OEM Solution Resellers who have not participated ItR Wave 1 - Part B, will be given an opportunity to provide feedback at a later date in the Solicitation process, and will be eligible to submit Offers.)

Following Wave 1, the Final CBSOS is issued which includes the conditions outlining industry participation, and mechanisms for evaluating proposed Solutions and Resellers.

1.4 CBSOS Stages - Infographic



Stage 1: CBSOS- Initial

The Notice of Proposed Procurement (NPP) and CBSOS - Initial is published on Buyandsell.gc.ca.

Stage 2: Bilingual Information Webinar

Offerors are invited to attend a Bilingual Information Webinar. During the webinar, Canada will provide an overview of the approach, explain the ItR "waves", and gather feedback from industry on the proposed Solicitation process and evaluation framework.

Stage 3: ItR - Wave 1 (Part A & B)

During ItR - Wave 1 (Part A & B), Offerors are invited to provide feedback and share their perspectives by participating in various interactive events facilitated by Canada. Offeror's feedback and presentations will not be scored nor considered in the Solicitation evaluation process, ItR questions and answers will be documented. The purpose of the ItR - Wave 1 (Part A & B) is to help Canada characterize what industry has to offer, to help Canada determine the best way to leverage Resellers at the Contract stage, and to finalize the CBSOS. At Canada's discretion, additional ItR events (in the presence of all Offerors or "one-on-one") may be scheduled for the same purpose as outlined above.

Stage 4: CBSOS - Final

At Stage 4, based on observations during the ItR session(s), Canada will refine and issue the Final Challenge-Based Standing Offer Solicitation, beginning Component 2 of the Solicitation process. ItR participants may be invited to feedback sessions, designed to contribute to the improvement of the Agile Procurement process (PP3.0) framework.

Stage 5A: Solicitation Closing – SP/OEM

SP/OEM Offerors submit an Offer using Annex [X] - Offer Submission Form and Attachment [X] - Financial Offer Form. Unlike traditional procurement, Offerors are not required to provide a comprehensive written technical offer at Offer Closing. Refer to the paragraph entitled *Submission of Written Documents by Offerors*, of Section 3 - Offer Preparation Instructions, for information on the submission of written documents by Offerors.

Stage 5B: Demonstration - SP/OEM

SP/OEM Offerors that are compliant with the mandatory procedural requirements and the Mandatory Financial Evaluation Criteria described herein are requested to make a demonstration.

Stage 5C: Notification of Selection - SP/OEM

The highest ranked SP/OEM Offerors following the Evaluation Procedures and Basis of Selection process (Section 4 of the CBSOS) are notified (Notification of Selection) of Canada's intent to award Standing Offers.

Stage 6A: Solicitation Closing - SP/OEM Solution Resellers

SP/OEM Solution Resellers submit an Offer using Annex [X] - Offer Submission Form and Attachment [X] - Financial Offer Form. Unlike traditional procurement, Offerors are not required to provide a comprehensive written technical offer at Offer Closing. Refer to the paragraph entitled *Submission of Written Documents by Offerors*, of Section A3 - Offer Preparation Instructions, for information on the submission of written documents by Offerors.

Stage 6B: Notification of Selection - SP/OEM Solution Resellers

The highest ranked SP/OEM Solution Resellers following the Evaluation Procedures and Basis of Selection process (Section 4 of the CBSOS) are notified (Notification of Selection) of Canada's intent to award Standing Offers.

Stage 7: Technical Offer

Offerors notified of selection at Stages 5C & 6B of Canada's intent to award Standing Offers are requested to submit their Technical Offer.

(Note to Offerors: Offeror's Technical Offers are not to be provided at Offer Closing, i.e., Stages 5A & 6A)

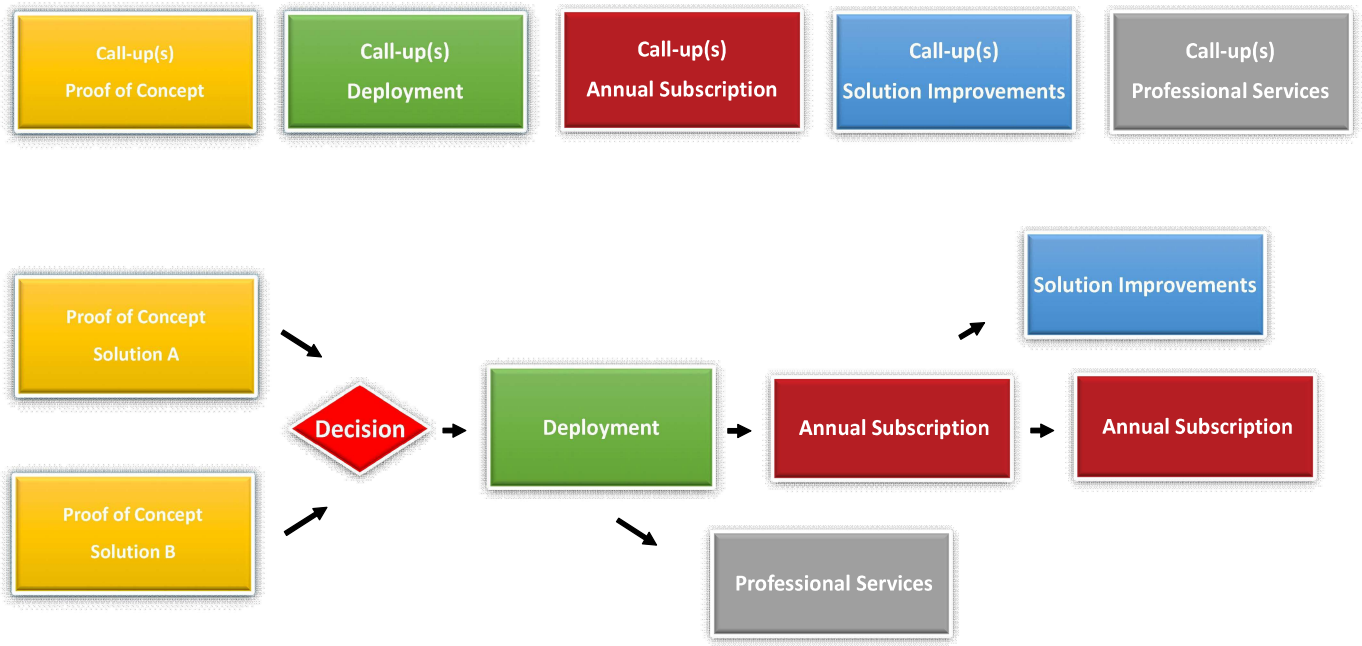
Stage 8: Standing Offer Award – WS 1 Call-ups (Proof of Concept)

Canada anticipates awarding multiple Standing Offers. At Standing Offer award, the Standing Offer Authority will issue a Call-Up Instrument for WS 1 - Proof of Concept to the Offerors holding a Standing Offer (Offer Holders) to develop, test, and evaluate selected Solutions i.e., proof of concepts in parallel. The proof of concept development, testing, and evaluation phase has an expected duration of 2 months, and a maximum Total Estimated Cost of $25,000, Applicable Taxes included.

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

This infographic is a visual representation of the Statement of Challenge Work Segments, and corresponding Work Segment Call-ups.

Work Segments/Call-ups - Infographic



WS 1 Call-ups - Proof of Concept

The Standing Offer Authority may issue WS 1 Call-ups - Proof of Concept to develop, test, and evaluate selected Solutions i.e., proof of concepts in parallel.

WS 2 Call-ups

a) Deployment of the Operational Solution

The Standing Offer Authority may issue WS 2 Call-ups to deploy the Operational Solution(s) for one or more Clients.

SSC is a federal government department that acts as a shared services organization. SSC will use the Solution(s) resulting from the CBSOS to provide a Solution(s) to one or more of its Clients. The initial lead Client will be [To be Determined], and SSC may select other Clients to use the Solution(s), for example, for further testing of the Solution. SSC's Clients include SSC itself, those government institutions for whom SSC's services are mandatory, and those other organizations for whom SSC's services are optional and that choose to use those services from time to time. In addition to the Government of Canada SSC may also serve a government of a province or municipality in Canada, a Canadian aid agency, a public health organization, an intergovernmental organization, or a foreign government.

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

- Deployment of the Operational Solution
- Annual Subscription Licenses
- Additional User Licenses

b) Call-ups - Solution Improvements

The Standing Offer Authority may issue Call-ups, for Solution(s) Improvements.

c) Call-ups - Professional Services

The Standing Offer Authority may issue Call-ups - Professional Services to require the Offeror to provide the Professional Services listed in Attachment A - Statement of Challenge (SoC), section entitled *Professional Services*.

(Note to Offeror: Call-ups - Professional Services may or may not be incorporated into the resulting Contract. The final CBSOS will include the applicable Work Segments (WS) and associated Standing Offer Call-ups.)

d) Call-ups - Catch-All

The Standing Offer Authority may issue Catch-All Call-ups to require the Offeror to provide any non-listed items that are or may be intended, in their entirety or in part, for the Cloud Security Services project(s).

1.6 Choice of Solutions

During the Proof of Concept work segments various Solutions will be compared. Based on favourable testing and evaluation results, from the Proof of Concept development, testing, and evaluation stage, Canada may select Solution(s) to be deployed (WS 2 Call-ups - Deployment). While the decision to issue WS 2 Call-ups - Deployment is entirely within Canada's discretion, it will do so in accordance with the Attachment A - Statement of Challenge paragraph, entitled *Decision-Making Framework for Choosing Solution(s) to be Deployed*.

Following the selection of Solution(s) to be Deployed, Canada may, by sending written notice to the Offeror, exercise its right, in its sole discretion, to suspend or set aside the Standing Offer for the convenience of the Crown.

1.7 Financial Capability Assessment

At Standing Offer award, Canada may conduct a complete financial capability assessment of the Offeror. Canada may request from the Offeror any financial information that Canada may require to conduct the assessment, which may include, but is not limited to, audited financial statements, if available, or unaudited financial statements (prepared by the Offeror's outside accounting firm, if available, or prepared in-house if no external statements have been prepared) for the Offeror's last three fiscal years, or for the years that the Offeror has been in business if this is less than three years. The financial statements must include, at a minimum, the Balance Sheet, the Statement of Retained Earnings, the Income Statement, and any notes to the statements.

1.8 Security Requirements

(Note to Offerors: in addition to the security requirements outlined in the section entitled *Cloud Security Requirements (Attachment A1)*, finalized Security Requirements will be set out in the Final Challenge-Based Standing Offer Solicitation.)

[Delete entire Sub-section if there are no security requirements.] The following security requirements must be met ["by the date of Offer Closing" or "by the date of Standing Offer award" or "prior to Canada issuing WS 1 Call-ups - Proof of Concept"].

[Insert Security Clearance Article(s) as determined with Technical Authority, CITS and PWGSC CISD.]

[Delete if N/A.] Attachment [X] - Security Requirements Check List refers.

[Delete if N/A.] In addition to these requirements, there are specific Client-driven security requirements at one or more sites where the Work will be performed, which are detailed in Attachment [X] Annex [X] Site-Specific Security Requirements.

1.9 Cloud Security Requirements

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

(Note to Offerors: a finalized General Information section will be set out in the Final Challenge-Based Standing Offer Solicitation.)

SECTION 2 - OFFEROR'S INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the CBSOS 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.

Offerors who submit an Offer agree to be bound by the instructions, clauses and conditions of the CBSOS and accept the clauses and conditions of the resulting Standing Offer.

2.2 Standard Instructions

SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services – Competitive Requirements are incorporated by reference into and form part of this CBSOS, and are amended as follows.

a) Where "Request for Standing Offer (RFSO)" appears:

Delete: in its entirety

Insert: "Challenge-Based Standing Offer (CBSOS)"

b) 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."

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

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

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

d) At section 08: *Transmission by facsimile or by epost Connect*:

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 RFSO process, enquiries and other communications regarding the RFSO must be directed only to the Standing Offer Authority identified in the RFSO. Failure to comply with this requirement may result in the offer being declared non-responsive."

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

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

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

The information exchanged between participants during the Invitation to Refine waves will be published, on a timely basis, in reports or presented during events called "What We Heard." The documentation associated with those reports or events will be uploaded to Buyandsell.gc.ca

Official information that is binding upon Canada will only be made available by the Point of Contact on Buyandsell.gc.ca

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

g) At section 14, *Price justification*:

Delete: "In the event that the Offeror's offer is the sole responsive offer received, the Offeror must provide, on Canada's request, one or more of the following price justification:"

Insert: "the Offeror must provide, on Canada's request, one or more of the following price justification:"

All references contained within the SACC 2005 (2017-06-21), General Conditions - Standing Offers - Goods or Services, to the Minister of Public Works and Government Services will be interpreted as a reference to the Minister of Digital Government presiding over Shared Services Canada and all references to the department of Public Works and Government Services will be interpreted as a reference to Shared Services Canada.

2.3 Consideration of Additional Terms

Acceptance of all the terms and conditions contained in Section 5 - Standing Offer and Section 6 - Resulting Contract Clauses (including those relating to software licensing and those incorporated by reference) are a mandatory requirement of this Solicitation.

However, Offerors may propose **no later than October 30th at 15:00 EST** additional T&Cs to Canada for consideration. Requests for consideration of additional T&Cs that do not meet this time limit will not be considered for inclusion in any Standing Offer and Resulting Contract Clauses.

Whether or not any proposed additional T&Cs are acceptable to Canada and subsequently included in the Standing Offer and Resulting Contract Clauses is a matter solely within the discretion of Canada, and will be determined in accordance with the following procedures.

A2.3.1. Offerors submit only to the Point of Contact, additional T&Cs that are proposed to supplement the Standing Offer and Resulting Contract Clauses. Offerors should not submit a software publisher's full standard license terms (because full standard license terms generally contain provisions that deal with more than simply how the software can be used; for example, they frequently deal with issues such as limitation of liability or warranty, neither of which are software use terms).

A2.3.2 Canada will review the Offeror's additional T&Cs, that are proposed to supplement the Standing Offer and Resulting Contract Clauses, to determine if there are any proposed additional T&Cs that are acceptable to Canada.

A2.3.3 If Canada determines that there are proposed additional T&Cs that are acceptable to Canada, the acceptable T&Cs will be included in the Standing Offer and Resulting Contract Clauses of the Final CBSOS released at Stage 6.

A2.3.4 If Canada determines that any proposed additional T&Cs are not acceptable to Canada, Canada will notify the Offeror in writing.

2.4 Enquiries - Solicitation

Questions and comments about this Solicitation can be submitted in accordance with SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services – Competitive Requirements, section 13 *Communication – solicitation period*, there will be two (2) question periods, as follows.

Question Period 1 (Wave 1): All enquiries are requested to be submitted in writing to the Point of Contact no later than three (3) calendar days before the Bilingual Information Webinar, and no later than three (3) calendar days before each Invitation to Refine event. Enquiries received that do not meet this condition may not be answered during the Information Webinar or during the Invitation to Refine event.

Question Period 2 (Invitation to Participate - SP/OEM): All enquiries are requested to be submitted in writing to the Point of Contact **no later than October 8 at 15:00 EST**. Enquiries received that do not meet this condition may not be answered before the Closing Date and Time for receipt of the Invitation to Participate Form. Enquiries received after that time will not be answered.

Offerors should reference as accurately as possible the numbered item of the Solicitation to which the enquiry relates. Care should be taken by Offerors 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 Offerors, so the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Offerors. Enquiries not submitted in a form that can be distributed to all Offerors may not be answered by Canada.

2.5 Point of Contact (PoC)

The Standing Offer Authority is the person designated by that title in the Solicitation, or by notice to the Offerors, to act as Canada's "Point of Contact" for all enquiries regarding the Solicitation process.

Name: Christopher Bromfield

Department: Shared Services Canada

Address: 180 Kent Street, Ottawa, ON K1G 4A8

Telephone Number: (343) 550-3959

Email Address: christopher.bromfield@ssc-spc.gc.ca

2.6 Offeror's Bilingual Information Webinar

An optional Offeror's Bilingual Information Webinar will be held on the following dates and times:

The Bilingual Webinar will be held on September 29, 2021 at 14:30 EST.

Join the Microsoft Teams Meeting here:

Microsoft Teams Meeting
Join on your computer or mobile app.
Click Here to Join the Meeting
Or call in (audio only)
Phone Conference Number: **1-343-803-4324** (Ottawa-Hull, Canada)
Phone Conference ID: **905 442 429#**

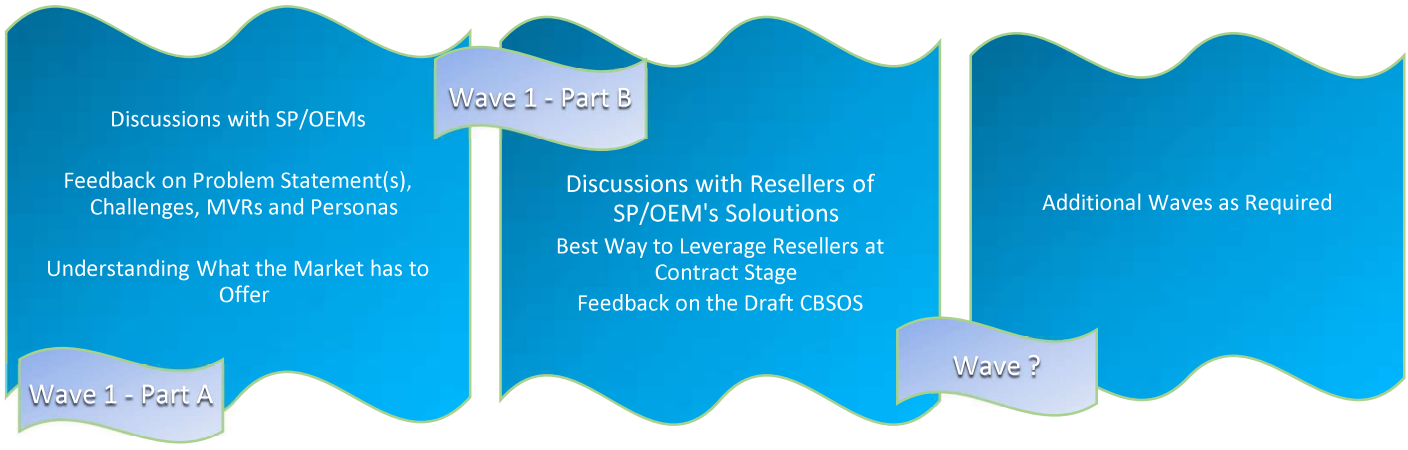
The scope of the Requirement outlined in this CBSOS will be reviewed during the Webinar and questions will be answered. It is recommended that Offerors who intend to submit an Offer participate in the Webinar. Offerors who do not attend the Webinar will not be prohibited from submitting an Offer. Information Webinar questions and answers will be documented. Based on the feedback received during the Webinar, Canada may refine and amend, or reissue the Solicitation.

At Canada's discretion, additional Information Webinars may be scheduled for the same purpose as outlined above. Logistical details will be published as an amendment to the CBSOS.

For reference purposes Offeror's Information Webinars are recorded.

2.7 Invitation to Refine

Invitation to Refine Waves



Up to 10 SP/OEM Offerors will be invited to provide feedback on the problem statement(s) and share their perspectives by participating in various interactive events (videoconferences, group interactions, surveys) facilitated by Canada (in the presence of all Offerors or "one-on-one"). Offerors may be invited to make a presentation of their Solution, explaining how their Solution could resolve the problem statement(s).

SP/OEM Solution Resellers will be invited to provide feedback in order to help Canada determine the best way to leverage Resellers at the Contract stage, and to help Canada finalize the CBSOS.

Offeror's feedback and presentations (if applicable) will not be scored nor considered in the Solicitation evaluation process, ItR questions and answers will be documented. At Canada's discretion, additional ItRs events (in the presence of all Offerors or "one-on-one") may be scheduled for the same purpose as outlined above.

2.7.1 Current ItR Events Schedule

- ItR - Wave 1 (Part A) SP/OEM: October 18, 2021 to November 5, 2021
- ItR - Wave 1 (Part B) SP/OME Solution Resellers: October 18, 2021 to November 5, 2021

2.7.2 Registration for Invitation to Refine Events

(Wave 1 - Part A) SP/OEM

To participate in **ItR - Wave 1 (Part A)**, SP/OEMs are requested to confirm their intention to participate in the Invitation to Refine events by sending an email to PoC at: christopher.bromfield@ssc-spc.gc.ca no later than **October 4, 2021 at 15:00 EST.** OEMs may end their participation at anytime.

Following receipt of their intention to participate, **(ItR - Wave 1 (Part A)** the PoC will email a "unique identifier number (UID)" and a link to the Invitation to Participate Form.

To participate in **ItR - Wave 1 (Part A)**, OEMs **must submit their Invitation to Participate Form** no later than **October 13, 2021 at 15:00 EST.**

SP/OEMs are requested to include in the confirmation of their intention to participate in the Invitation to Refine events, the following:

- name of the Organization;
- Organization telephone number;
- The name of the main representative of the organization who will act as the point of contact and who will participate in the events;
- name of each of the Organization's Other Representatives who will be attending the ItR events;
- email address of each of the Organization's Representatives who will be attending the ItR events including the one of the organization's point of contact;
- an Official Language preference.

(Wave 1 - Part B) SP/OME Solution Resellers

Resellers are requested to confirm their intention to participate in the Invitation to Refine events by sending an email to PoC at: christopher.bromfield@ssc-spc.gc.ca

To participate in the **ItR - Wave 1 (Part B)**, Resellers should register no later than **October 4, 2021 at 15:00 EST**. Resellers may end their participation at anytime.

Following receipt of their intentions to participate, **(ItR - Wave 1 (Part B)** the PoC will email an official invitation including logistical details to Registrants.

Resellers are requested to include in the confirmation of their intention to participate in the Invitation to Refine events, the following:

- name of the Organization;

- Organization telephone number;
- The name of the main representative of the organization who will act as the point of contact and who will participate in the events;
- name of each of the Organization's Other Representatives who will be attending the ItR events;
- email address of each of the Organization's Representatives who will be attending the ItR events including the one of the organization's point of contact;
- an Official Language preference.

(Note to Offerors: The "rules of engagement" for the ItR events will be presented to Offerors during the Information Webinar. By participating in the ItR events, Offeror's consent to these rules of engagement.)

2.8 Window of Opportunity for Underrepresented Groups (URG) including Small and Medium Enterprises (SMEs)

Under Agile Procurement Process 3.0, Underrepresented Groups and Small and Medium Enterprises are invited to network with industry and government through participatory processes, e.g., Webinars, and Invitation to Refine events.

The primary goals of these participatory processes are:

- to create opportunities for URGs and SMEs to achieve active participation in the Solicitation process;
- to be "seen" by industry participants;
- to help URGs and SMEs identify shared interest as well as creative and innovative ideas;
- to forge possible alliances with other industry members participating in the Solicitation process;
- to create opportunities for URGs and SMEs to participate as "Offerors" in the Solicitation process.

Mechanism for participation beyond the Invitation to Refine wave will be specified in the Final CBSOS.

2.9 Applicable Laws

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

Offerors may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their Offer, by inserting the name of the Canadian province or territory of their choice in Annex [X] - Offer Submission Form. If no change is made, the Offeror acknowledges that the applicable laws specified are acceptable to the Offeror.

2.10 Trade Agreements

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

Canadian Free Trade Agreement (CFTA) Canada-Colombia Free Trade Agreement Canada-Korea Free Trade Agreement Canada-Ukraine Free Trade Agreement	Canada-Chile Free Trade Agreement Canada-European Union Comprehensive Economic and Trade Agreement (CETA) Canada-Panama Free Trade Agreement	Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Canada-Honduras Free Trade Agreement Canada-Peru Free Trade Agreement

	World Trade Organization - Agreement on Government Procurement (WTO-GPA)	

2.11 Certifications Precedent to Standing Offer Award and Additional Information

The certifications and additional information should be submitted using Annex [X] - Offer Submission Form. If any of the required certifications or additional information is not complete and submitted as requested, the PoC will inform the Offeror, by sending a written notice of a time frame within which to comply with the request. Failure to comply with the request within the time frame specified will render the Offer non-responsive.

The certifications provided by Offerors to Canada are always subject to verification by Canada. Unless specified otherwise, Canada will declare an Offer non-responsive, or will declare a Contractor in default if any certification made by an Offeror is found to be untrue, whether made knowingly or unknowingly, whether in its Offer, during the Offer evaluation period, or during the Standing Offer period.

The Point of Contact will have the right, by sending a written notice to the Offeror at any time, to request additional information to verify the Offeror's certifications. Failure to comply with this request will render the Offer non-compliant or will constitute a default under any Call-up that may be issued as a result of the Solicitation process.

(Note to Offerors: a finalized Offeror Instruction section will be set out in the Final Challenge-Based Standing Offer Solicitation.)

SECTION 3 - OFFER PREPARATION INSTRUCTIONS

(Note to Offerors: a finalized Offer Preparation Instructions section will be set out in the Final Challenge-Based Standing Offer Solicitation.)

SECTION 4 – EVALUATION PROCEDURES AND BASIS OF SELECTION

(Note to Offerors: a finalized Evaluation Procedures and Basis of Selection section will be set out in the Final Challenge-Based Standing Offer Solicitation.)

SECTION 5 & 6 - STANDING OFFER AND RESULTING CONTRACT CLAUSES

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

No modification to the Standing Offer terms and conditions included in the Offeror's Offer will apply to the resulting Standing Offer, even though the Offer may become part of the resulting Standing Offer.

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

Offerors submitting Offers containing statements implying that the Offer is conditional on modification to these Standing Offer terms and conditions (including all documents incorporated into the Standing Offer by reference) or containing terms and conditions that purport to supersede these Standing Offer terms and conditions will be considered non-responsive. As a result, Offerors with concerns regarding the Standing Offer terms and conditions should raise those concerns in accordance with the paragraph entitled *Enquiries - Solicitation* of the CBSOS.)

SECTION 5 STANDING OFFER

(Note to Offerors: the Standing Offer will be customized in accordance with the Final CBSOS prior to Standing Offer award.)

5.1 Offer

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

5.2 Series of Standing Offers

The Offeror acknowledges that this Standing Offer is one of a series of [insert #] Standing Offers awarded as a result of the Challenge-Based Standing Offer Solicitation, issued by Canada on [insert release date] under Solicitation No. [insert #].

The award of this Standing Offer begins Work Segment 1 of the overall Cloud Security Services initiative described in the Solicitation.

Throughout Work Segment 1 (Proof of Concept), awarded Standing Offers will be utilized concurrently, forming a procurement ecosystem.

The Proof of Concept Work Segment has an expected duration of [insert #] months.

Canada will advise all Offerors, at the end of the Proof of Concept Work Segment, of its intention to proceed to Work Segment 2 - Deployment of the Operational Solution.

5.3 Standing Offer Award and Work Segment 1 Call-ups - Proof of Concept

In conjunction with Standing Offer award, the Standing Offer Authority may issue Work Segment 1 Call-ups - Proof of Concept, to develop, test, and evaluate the Solution.

5.3.1 Work Segment 1 Call-ups - Proof of Concept

The Offeror must deliver the [insert name of Solution] Proof of Concept and perform all the Work in accordance with the terms and conditions of any Work Segment 1 Call-up(s), this Standing Offer, including Attachment A - Statement of Challenge, and the Contractor's Technical Offer entitled [insert name of Offer], dated [insert date], and in accordance with the prices set out in the Attachment [X] - Basis of Payment.

5.3.1.1 Fairness and Transparency Platform

To ensure procedural fairness, the following will be implemented.

5.3.1.2 Testing Process

The Testing Process is outlined in Attachment A - Statement of Challenge (SoC).

5.3.1.3 Canada's Commitment(s) During Work Segment 1

- Throughout Work Segment 1, Canada commits to sharing any information material to the choice of the Solution to be deployed, in a timely and equal manner, with all Offerors participating in the procurement ecosystem.
- Throughout Work Segment 1, Canada commits to disclose any Non-compulsory Additional Functionalities that Canada has become aware of and interested in exploring, in a timely and equal manner, to all Offerors participating in the procurement ecosystem.

5.3.1.4 Value for Money

Canada reserves the right, in its sole discretion, to add "found" Non-compulsory Additional Functionalities to the Solution. The Offeror will be responsible for demonstrating value for money for any Non-compulsory Additional Functionality Canada chooses to add to the Solution.

Canada may contract an independent expert to validate and advise Canada on the Solution's pricing components including "found" Non-compulsory Additional Functionality to the Solution. The independent expert's findings will be made available to the specific Offeror.

5.3.1.5 Choice of the Solution(s) to be Deployed (Work Segment 2)

Canada will, in a timely and equal manner, inform all Offerors in the procurement ecosystem of which Operational Solution(s) is to remain available for Call-up Allocation. Following the completion of the Proof of Concept, Canada may, by sending written notice to the Offeror, exercise its right, in its sole discretion, to retain, suspend or set aside the Standing Offer.

5.4 Work Segments - Standing Offer Call-ups

The following Work Segments (WS) and associated Call-ups are available to Canada under this Standing Offer.

- WS 1 Call-ups - Proof of Concept
- WS 2 Call-ups - Deployment of the Operational Solution

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

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

5.4.1 WS 1 Call-ups - Proof of Concept

The Standing Offer Authority may issue WS 1 Call-ups - Proof of Concept to develop, test, and evaluate the Offeror's Solution, in accordance with the paragraph entitled *Standing Offer Award and WS 1 Call-ups - Proof of Concept*.

5.4.2 WS 2 Call-ups - Deployment of the Operational Solution on Shared Services Canada's Operational Environment

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

The Standing Offer Authority may issue WS 2 Call-ups to require the Offeror to deploy the Operational Solution, in accordance with the terms and conditions of this Standing Offer.

Canada anticipates selecting [insert #] Offeror(s) to proceed with the Deployment of the Operational Solution on Shared Services Canada's Operational Environment. However, Canada may, in its discretion, issue WS 2 Call-ups to other Offerors at any time prior to the expiry date of the Standing Offer.

5.4.2.1 WS 2 Call-ups: Deployment on Additional Client's Operational Environments

The Standing Offer Authority may issue WS 2 Call-ups to require the Offeror to deploy the [insert name of Solution] Solution on Additional Client's Operational Environments, in accordance with the terms and conditions of this Standing Offer, including Attachment A - Statement of Challenge, and in accordance with the prices set out in Attachment [X] - Basis of Payment.

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

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

The Offeror acknowledges that Canada, prior to issuing WS 2 Call-ups, may request a price reduction to the prices set out in Attachment [X] - Basis of Payment, based on economies of scale. The Standing Offer Authority may request the Offeror submit a price breakdown showing, if applicable, the cost of direct

labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, markup, and any other supporting documentation.

The Standing Offer Authority may issue WS 2 Call-ups for Deployment on Additional Client's Operational Environments at any time after issuing WS 2 Call-ups - Deployment on Shared Services Canada's Operational Environment.

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

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

5.4.3 Call-ups - Solution Improvements

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

5.4.4 Call-ups - Professional Services

The Standing Offer Authority may issue Call-ups – Professional Services to require the Offeror to provide any resource(s) listed in Attachment A - Statement of Challenge, paragraph entitled, *Professional Services.*

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

Is incorporated into the CBSOS by reference.

5.4.5 Call-ups – Catch All

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

5.5 Call-up Instrument and Procedures

5.5.1 Call-up Instrument

The Work will be authorized or confirmed by the Standing Offer Authority using the duly completed Call-up Instrument - Attachment [X] which shall contain at a minimum the following information:

- standing offer number;
- statement that incorporates the terms and conditions of the Standing Offer;
- description and unit price for each line item;
- total value of the call-up;

- point of delivery;
- confirmation that funds are available under section 32 of the Financial Administration Act;
- confirmation that the user is an Identified User under the Standing Offer with authority to enter into a contract.

(Note to Offerors: the Call-up Instrument - Attachment [X], will be set out in the Final Challenge-Based Standing Offer Solicitation.)

5.5.2 Call-up Procedures

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

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

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

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

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

The Work will be for a Firm Price; however, whenever the Work cannot be well defined, in lieu of a Firm Price, the Project Authority may pre-authorize a time rate payment, i.e., per diem rates, in accordance with the Professional Services (Type 1) of Attachment [X] - Basis of Payment.

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

5.5.3 Limitation of Call-ups

Individual Call-ups against the Standing Offer must not exceed $ [insert amount] (Applicable Taxes included).

5.6 Standing Offer Call-up Allocation Method (CAM)

(Note to Offerors: subsequent to the Proof of Concept, a "Best Fit" Call-up Allocation Method (CAM), will be used to authorize Call-ups under the Standing Offer.)

Canada will use elements from the Demonstration Evaluation Criteria, and decision-making framework, to identify the strengths and limitation of each Offeror's Solution. Client departments (Users) will select the right Solution "Best Fit" that meets their business goals, by taking into account the Solution's strengths and limitations.

5.7 Standing Offer Reporting - Standing Offer Holders

The Offeror must compile and maintain records on its provision of goods, services or both to Canada under Call-ups resulting from the Standing Offer. Whether or not the Offeror's Standing Offer usage reports are acceptable to Canada is determined entirely within the discretion of Canada. If Canada

determines that the Offeror's reports do provide sufficient data, the PoC will, by sending a written notice to the Offeror, request that the Offeror correct their usage reports within any time specified in the notice.

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

The data must be submitted on a quarterly basis, no later than 15 calendar days after the end of the quarterly report period. The quarterly reporting periods are defined as follows:

Quarterly Reporting Periods

Quarter	Period Covered	Due on or Before
1st	April 1 to June 30	July 15
2nd	July 1 to September 30	October 15
3rd	October 1 to December 31	January 15
4th	January 1 to March 31	April 15

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

5.8 Challenge-Based Standing Offer Holders List - Refresh

Subsequent to the establishment of the Standing Offer Holders List, and throughout the period of the Standing Offer, Canada may, at its sole discretion, and at any point during the Standing Offer validity period, re-post the CBSOS on Buyandsell.gc.ca.

This would permit additional Vendors/Firms to qualify and to be added to the Standing Offer Holders List, and to allow existing Standing Offer Holders to submit proposals to modify their existing Standing Offer.

Offers will be subject to the same qualification requirements as those required in the original CBSOS, Solicitation No.: [insert CBSOS Solicitation #].

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

5.9 Suspension or Set Aside of Standing Offer by Canada

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

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

5.10 Standing Offers Reporting - Standing Offer Users

(Note to Offerors: the Standing Offer Reporting - Standing Offer Users provisions will be set out in the Final Challenge-Based Standing Offer Solicitation.)

5.11 Standard Clauses and Conditions

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

5.11.1 General Conditions

The following General Condition is incorporated by reference.

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

[Delete entire Article if there are no approved additional terms and conditions.]

5.11.2 Additional Terms and Conditions - Approved by Canada

The Offeror acknowledges that the additional terms and conditions specifically set out in this paragraph have been approved by Canada, and that no additional terms and conditions included in the Offeror's Offer, or any terms and conditions incorporated into the Offeror's Offer by reference, will be binding upon Canada; even though the Offer may become part of the Standing Offer, unless they have been listed in the following paragraph.

5.11.2.1 [Insert if there are approved additional terms and conditions.] Approved (in accordance with the paragraph entitled *Consideration of Additional Terms* of the CBS) additional terms:

512 Security Requirements

[Delete entire Sub-section if there are security requirements.] There are no Security Requirements associated with this Solicitation.

[Delete entire Sub-section if there are no security requirements.] The following security requirements must be met ["by the date of Offer Closing" or "by the date of Standing Offer award" or "prior to Canada issuing any Call-up Instrument against the Standing Offer"].

[Insert Security Clearance Article(s) as determined with Technical Authority, CITS and PWGSC CISD.]

[Delete if N/A.] Attachment [X] - Security Requirements Check List refers.

[Delete if N/A.] In addition to these requirements, there are specific Client-driven security requirements at one or more sites where the Work will be performed, which are detailed in Attachment [X] Annex [X] Site-Specific Security Requirements.

5.13 Cloud Security Requirements

5.13.1 Cloud Service Provider - Security Requirements

(Note to Offerors: in addition to the security requirements outlined in the section entitled *Security Requirements*, Cloud Service Provider – Security Requirements provisions will be defined and set out in the Final Challenge-Based Standing Offer Solicitation.)

5.14 On-going Supply Chain Integrity (SCI) Process

(Note to Offerors: in addition to the Security requirements outlined in the section entitled *Security Requirements*, On-going Supply Chain Integrity (SCI) Process provisions will be defined and set out in the Final Challenge-Based Standing Offer Solicitation.)

5.15 Evolving Cyber Security Requirements (Evergreen)

As a result of the Standing Offer being perpetual, from time to time, SSC may also amend any Security Requirement provision outlined in any part of the Standing Offer as a result of a policy notification, legislation, procedural or technological change. Any such change will not affect existing contracts in place prior to the date of change. Notification of such change will be sent to Standing Offer Holder via a generic email. Should a Standing Offer Holder not agree with such modifications, and no longer wishes to be considered for requirements issued under the Standing Offer framework as a result of the changes, the Standing Offer Holder will notify the Standing Offer Authority and this Standing Offer Holder will no longer be on the list of Standing Offer Holders.

5.16 Data Ownership and Sovereignty

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

a) it, its employees, representatives, and agents are prohibited from accessing the content transmitted by the Solution at any time without the written consent of the Standing Offer Authority; and
b) it is prohibited from permitting any third party to access the content transmitted by the Solution at any time without the written consent of the Standing Offer Authority.

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

5.17 Term of Standing Offer

5.17.1 Period of the Standing Offer

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

Canada may, by notice in writing to all Standing Offer Holders and by posting on Buyandsell.gc.ca, cancel this Standing Offer by giving all Standing Offer Holders at least 30 calendar days' notice of the cancellation.

5.17.2 Changes to the Standing Offer (Evergreen Clause)

As a result of the Standing Offer being perpetual, from time to time, SSC may also amend any part of the Standing Offer as a result of, but not limited to, a policy notification, legislation, or procedural change. Any such change will not affect existing contracts in place prior to the date of change. Notification of

such change will be sent to Standing Offer Holder via a generic email. Should a Standing Offer Holder not agree with such modifications, and no longer wishes to be considered for requirements issued under the Standing Offer framework as a result of the changes, the Standing Offer Holder will notify the Standing Offer Authority and this Standing Offer Holder will no longer be on the list of Standing Offer Holders.

5.17.3 Delivery Points

Delivery will be made to delivery point(s) specified at Attachment A - Statement of Challenge.

5.18 Authorities

5.18.1 Standing Offer Authority

The Standing Offer Authority for the Contract is:

(Note to Offerors: this information will be completed at Standing Offer award.)

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

5.18.2 Project Authority

The Project Authority for the Standing Offer is:

(Note to Offerors: this information will be completed at Standing Offer award.)

The Project Authority is responsible for all matters concerning the technical content of the Work under the Standing Offer. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a Standing Offer amendment issued by the Standing Offer Authority.

5.18.3 Offeror's Representative

(Note to Offerors: this information will be completed at Standing Offer award.)

[insert Representative's name] _____ has been appointed as the representative for the Offeror and has full authority to act as agent for the Offeror regarding all matters relating to the Standing Offer.

[Delete entire Article if not a Joint Venture Offeror.]

5.18.4 Joint Venture

(Note to Offerors: this paragraph will be deleted if the Offeror awarded the Standing Offer is not a Joint Venture. If the Offeror is a Joint Venture, this clause will be completed with information provided in the Offeror's Offer.)

a) The Offeror confirms that the name of the Joint Venture is _____ and that it is comprised of the following members: [List all the Joint Venture members named in the Offeror's original proposal].

b) With respect to the relationship among the members of the Joint Venture Offeror, each member agrees, represents and warrants (as applicable) that:
   I. _____ has been appointed as the "representative" for the Joint Venture Offeror and has full authority to act as agent for each member regarding all matters relating to the Offer;
   II. by giving notice to the representative, Canada will be considered to have given notice to all the members of the Joint Venture Offeror; and
   III. all payments made by Canada to the representative will act as a release by all the members.
c) All the members agree that Canada may terminate the Offer in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.
d) All the members are liable jointly and severally or solidarily for the performance of the entire Offer.
e) The Offeror acknowledges that any change in the membership of the Joint Venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment terms and conditions of the General Conditions.
f) The Offeror acknowledges that all security and controlled goods requirements in the Offer, if any, apply to each member of the Joint Venture Offeror.

5.19 Identified Users

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

5.20 Price Adjustment Mechanism

At the request of the Offeror, the prices for Call-ups issued twenty-four (24) months after the date of Standing Offer award, will be adjusted in accordance with the following Price Adjustment Mechanism. The prices will be adjusted to account for inflation according to Table 18-10-0004-01 Consumer Price Index, monthly, not seasonally adjusted, All-items, Canada

New Price =

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

For example:

The initial price for a Requirement - Work Segment 2 Call-ups is $ 1000.
Standing Offer award March 31, 2019.
A Work Segment 3 Call-up for a deployment requirement on additional Client's operational environment is issued on June 2, 2021.
CPI for March 2019 = 134 (hypothetical value)
CPI for May 2021 = 136
The new price = 1000 * (1+ (136-134) / 134) = $ 1,014.93

5.21 Exchange Rate Fluctuation

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

a) From Standing Offer award to invoice payment(s), if raised by Canada or the Offeror, Canada will adjust the price(s), as specified in Attachment [X] - Basis of Payment, to reflect the exchange rate fluctuation, in Canadian dollars (CAD), if the exchange rate fluctuation is greater than 8% (increase or decrease) from the date of Standing Offer award. If either of the aforementioned dates fall on a Saturday, Sunday or statutory holiday (non-Federal Government Working Days), Canada will calculate the rate using the previous workday. The exchange rate adjustment amount will be calculated in accordance with the following formula:

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

b) The initial exchange rate (CAD) is set as the daily average rate as published by the Bank of Canada on the Offer Closing date.
c) Canada reserves the right to audit any price adjustments in accordance with the Accounts and audit provisions of the *SACC 2035 (2020-05-28), General Conditions - Higher Complexity - Services.*
d) This clause will only apply to the goods and services directly impacted by the exchange rate e.g., hardware, software, and certain operational maintenance and support services.

5.22 Financial Limitation Total

The total cost to Canada resulting from Call-ups against the Standing Offer must not exceed the sum of $ [insert $ amount] (Applicable Taxes excluded) unless otherwise authorized in writing by the Standing Offer Authority. The Offeror must not perform any Work or services or supply any articles in response to Call-ups which would cause the total cost to Canada to exceed the said sum, unless an increase is so authorized.

The Offeror must notify the Standing Offer Authority as to the adequacy of this sum when 75 % of this amount has been committed, or four months before the expiry date of the Standing Offer, whichever comes first. However, if at any time, the Offeror considers that the said sum may be exceeded, the Offeror must promptly notify the Standing Offer Authority.

5.23 Direct Request by Customer Department

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

Is incorporated into the CBSOS by reference.

5.24 Taxes - Foreign-based Contractor

[Use the following clause in Standing Offers when an Offer may be received from a foreign-based contractor.]

SACC C2000C (insert date), Taxes - Foreign-based Contractor

Is incorporated into the CBSOS by reference.

5.25 Certifications of Compliance

Compliance with the Certifications provided by the Offeror is a condition of authorization of the Standing Offer and subject to verification by Canada during the entire period of the Standing Offer

and of any resulting Contract that would continue beyond the period of the Standing Offer. In the event that the Offeror does not comply with any certification or that it is determined that any certification made by the Offeror in its Offer is untrue, whether made knowingly or unknowingly, the Standing Offer Authority has the right to terminate any resulting Contract for default and set aside the Standing Offer.

5.26 Applicable Laws

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

(Note to Offerors: this information will be completed at Standing Offer award.)

5.27 Foreign Nationals

[Use the following clause in Standing Offers for goods and services with a Canadian Offeror where there could be a need for the Offeror to hire foreign nationals (i.e., non-Canadians or non-permanent residents) to work in Canada.}

SACC A2000C (insert date) Foreign Nationals (Canadian Contractor)

Is incorporated into the CBSOS by reference.

Or

[Use the following clause in Standing Offers for goods and services with a foreign Offeror where there could be a need for the Offeror to hire foreign nationals (i.e., non-Canadians or non-permanent residents) to work in Canada.]

SACC A2001C (insert date) Foreign Nationals (Foreign Contractor)

Is incorporated into the CBSOS by reference.

5.28 Insurance – No Specific Requirement

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

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

First Party Liability

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

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

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

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

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

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

5.30 Safeguarding Electronic Media

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

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

5.31 Priority of Documents

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

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

a) the Call-up against the Standing Offer, including any Attachments and Annexes;
b) the Standing Offer, including any attachments and annexes;
c) SACC 2005 (2017-06-21), General Conditions - Standing Offers - Goods or Services);
d) the Offeror's Offer dated _____ [insert date of offer], as amended on _____ [insert date(s) of amendment(s), if applicable], not including any software publisher license terms and conditions that may be included in the Offer, not including any terms and conditions in the Offer with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the Offer.

(Note to Offerors: a finalized Standing Offer section will be set out in the Final Challenge-Based Standing Offer Solicitation.)

SECTION 6 RESULTING CONTRACT CLAUSES

(Note to Offerors: the Resulting Contract Clauses will be customized in accordance with the Final Challenge-Based Standing Offer Solicitation prior to Standing Offer award.)

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

6.1 Statement of Challenge

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

6.2 Standard Clauses and Conditions

6.2.1 General Conditions

The following General Condition is incorporated by reference.

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

6.2.2 Supplemental General Conditions

(Note to Offeror: the following Supplemental General Conditions may or may not be incorporated into the resulting Contract. The final CBSOSwill include the applicable Supplemental General Conditions).

The following Supplemental General Conditions are incorporated by reference.

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

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

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

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

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

6.2.2.1 4003 Supplemental General Conditions - Licensed Software

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

Licensed Software	The Licensed Software, which is defined in 4003, includes all the products offered by the Contractor in its Offer, and any other software required for those products to function in accordance with the Software Documentation and the Specifications, including without limitation all of the following products: (Note to Offeror: this information will be completed at Standing Offer award using information from the Offeror's Offer.)
Type of License being Granted	[insert, User or Device or Entity] License, in accordance with section [insert 04, or 05, or 06] of 4003.
Language of Licensed Software	The Licensed Software must be delivered in [insert English or French or both].
Delivery Location	As specified in Attachment A - Statement of Challenge
Media on which Licensed Software must be Delivered	DVD, USB, or Internet link for download (including any file hash code)
Source Code Escrow Required	No

6.2.2.2 4004 Supplemental General Conditions - Maintenance and Support Services for Licensed Software

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

WS 2 Call-ups – Deployment: Operational Support and Maintenance Services & On-going Operational Support and Maintenance Services	(Note to Offeror: this information will be completed at Standing Offer award using information from the Offeror's Offer.)
Hours for Providing Hot Line Support Services	(Note to Offeror: this information will be completed at Standing Offer award using information from the Offeror's Offer.)
Contractor must keep track of software releases for the purpose of configuration control	(Note to Offeror: this information will be completed at Standing Offer award using information from the Offeror's Offer.)
Contact Information for Accessing the Contractor's Support Services	In accordance with section 05 *Support Services* of 4004, the Contractor will make its support services available through the following: • Toll-free Telephone Access: • Toll-free Fax Access: • Email Access: (Note to Offeror: this information will be completed at Standing Offer award using information from the Offeror's Offer.)
Website	In accordance with section 05 *Support Services* of 4004, the Contractor must make support services available over the Internet. To do so, the Contractor must include, as a minimum, frequently asked questions and on-line software diagnostic and support tools. Despite the Hours for Providing Hot Line Support Services, the Contractor's website must be available to Canada's users 24 hours a day, 365 days a year, and must be available 99% of the time. The Contractor's website address for web support is: (Note to Offeror: this information will be completed at Standing Offer award using information from the Offeror's Offer.)
Language of Support Services	The Support Services must be provided in both French and English, based on the choice of the User requesting support.
Section 07, paragraph 1 of 4004: *Canada's Responsibilities*	Canada will not maintain, for the software Support Period, a telephone line and Internet access for use in connection with the software support services.

6.3 Term of Contract

6.3.1 Period of the Contract

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

6.3.2 Delivery Date

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

6.4 Payment

6.4.1 Basis of Payment

6.4.1.1 Basis of Payment - Firm Price

WS 1 Call-ups - Proof of Concept

In consideration of the Contractor satisfactorily completing all of its obligations under the Contract, the Contractor will be paid the firm price; as specified in Attachment [X] - Basis of Payment, of [insert $ amount] Customs duties are included, and Applicable Taxes are extra.

6.4.1.2 Basis of Payment - Limitation of Expenditure

- WS 2 Call-ups - Deployment of the Operational Solution
- Call-ups - Professional Services

In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid as specified in Attachment [X] - Basis of Payment, to a limitation of expenditure of $ [insert $ amount]. Customs duties are included, and Applicable Taxes are extra.

6.4.1.3 Basis of Payment – Call-ups Solution Improvements

[Choose Option 1] In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid, for improvements that are provided by the Contractor itself, the prices determined in accordance with the applicable principles for price justification, found in SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services - Competitive Requirements subsection 14 *Price justification*.

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

Or

[Choose Option 2] In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid, for improvements that are provided by the Contractor itself, the prices determined in accordance with the applicable forms of price support.

Upon request by the Standing Offer Authority, the Contractor must submit the following forms of price support:

a) a current published price list and the percentage discount available to Canada (which must be commensurate with the discount for the other services already being provided to Canada);
b) paid invoices for similar goods or services (similar quality and quantity) sold to other customers; if the Contractor is required to keep the identity of its customers confidential, the Contractor may black out any information on these invoices that could reasonably reveal the customer's identity, as long as the Contractor provides, together with the invoices, a certification from its Senior Financial Officer with the profile of the customer (e.g., whether it is a public sector or private sector customer, the customer's size and service locations, and the nature of the goods and/or services it receives from the Contractor), in order to allow Canada to determine whether

the goods or services received by the customer are comparable to those Canada receives from the Contractor;

c) a price breakdown showing, if applicable, the cost of direct labour, direct materials, purchased items, engineering and plant overheads (if applicable), general and administrative overhead, transportation, profit, etc.;
d) a price certification from the Contractor and/or;
e) in accordance with the SACC 1031-2 (2012-07-16) Contract Cost Principles.

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

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

[Choose Option 1] In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid, for any non-listed items that are or may be intended, in their entirety or in part, for the [insert Project name] project, that are provided by the Contractor itself, the prices determined in accordance with the applicable principles for price justification, found in SACC 2006 (2020-05-28) Standard Instructions - Request for Standing Offers - Goods or Services - Competitive Requirements subsection 14 *Price justification*.

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

Or

[Choose Option 2] In consideration of the Contractor satisfactorily completing all its obligations under the Contract, the Contractor will be paid, for any non-listed items that are or may be intended, in their entirety or in part, for the [insert Project name] project, that are provided by the Contractor itself, the prices determined in accordance with the applicable forms of price support.

Upon request by the Standing Offer Authority, the Contractor must submit the following forms of price support:

a) a current published price list and the percentage discount available to Canada (which must be commensurate with the discount for the other services already being provided to Canada);
b) paid invoices for similar goods or services (similar quality and quantity) sold to other customers; if the Contractor is required to keep the identity of its customers confidential, the Contractor may black out any information on these invoices that could reasonably reveal the customer's identity, as long as the Contractor provides, together with the invoices, a certification from its Senior Financial Officer with the profile of the customer (e.g., whether it is a public sector or private sector customer, the customer's size and service locations, and the nature of the goods and/or services it receives from the Contractor), in order to allow Canada to determine whether the goods or services received by the customer are comparable to those Canada receives from the Contractor;

c) a price breakdown showing, if applicable, the cost of direct labour, direct materials, purchased items, engineering and plant overheads (if applicable), general and administrative overhead, transportation, profit, etc.;
d) a price certification from the Contractor and/or;
e) in accordance with the SACC 1031-2 (2012-07-16) Contract Cost Principles.

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

6.4.2 Method of Payment

(Note to Offeror: the following Method(s) of Payment may or may not be incorporated into the resulting Contract. The final CBSOSwill include the applicable Method(s) of Payment(s).

6.4.2.1 Single Payment

Canada will pay the Contractor upon completion and delivery of the Work, in accordance with Attachment [X] - Basis of Payment if:

I. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
II. all such documents have been verified by Canada;
III. the Work delivered has been accepted by Canada.

6.4.2.2 Monthly Payment

Canada will pay the Contractor monthly for Work performed during the month covered by the invoice, in accordance with Attachment [X] - Basis of Payment if:

I. an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
II. all such documents have been verified by Canada;
III. the Work performed has been accepted by Canada.

6.4.2.3 Progress Payments - General

Canada will make progress payments in accordance with Attachment [X] - Basis of Payment, no more than once a month, for cost incurred in the performance of the Work, up to [insert #] percent of the amount claimed and approved by Canada if:

I. an accurate and complete claim for progress payment and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
II. the amount claimed is in accordance with the basis of payment;
III. the total amount for all progress payments paid by Canada does not exceed [insert #] percent of the total amount to be paid under the Contract.

The balance of the amount payable will be paid in accordance with the payment provisions of the Contract upon completion and delivery of the Work if the Work has been accepted by Canada and a final claim for the payment is submitted.

Progress payments are interim payments only. Canada may conduct a government audit and interim time and cost verifications and reserves the rights to adjust the Contract from time to time during the performance of the Work. Any overpayment resulting from progress payments or otherwise must be refunded promptly to Canada.

6.4.2.4 Progress Payments - SMEs

Canada will make progress payments in accordance with Attachment [X] - Basis of Payment, no more than once a month, for cost incurred in the performance of the Work, up to ([insert %] % Committed $ for SMEs) of the amount claimed and approved by Canada if:

I. an accurate and complete claim for payment and any other document required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;
II. the amount claimed is in accordance with the Basis of Payment; and
III. the total amount for all progress payments paid by Canada does not exceed ([insert %] % Committed $ for SMEs) of the total amount to be paid under the Contract.

The balance of the amount payable will be paid at the completion of the Option period, in accordance with the payment provisions of the Contract upon completion and delivery of all Work required under the Contract if the Work has been accepted by Canada and payment to SMEs have been made.

Payments are interim payments only. Canada may conduct a government audit and interim time and cost verifications and reserves the rights to adjust the Contract from time to time during the performance of the Work. Any overpayment resulting from progress payments or otherwise must be refunded promptly to Canada.

6.5 Invoicing Instructions

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

By submitting invoices (other than for any items subject to an advance payment), the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for Work performed by subcontractors.

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

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

- the date;
- the Contractor name and address;
- the Destination
- Standing Offer number;
- financial codes, including GST or HST (as applicable) registration number;
- description of the Work;
- category(ies) of personnel and number of days worked;

- Firm Per Hourly Rate on which the total dollar amount of the invoice is based;
- the amount invoiced (exclusive of the Goods and Services Tax (GST) or Harmonized Sales Tax (HST) as appropriate) and the amount of GST or HST, as appropriate, shown separately;
- Client Reference Number (CRN);
- Business Number (BN); and
- total value billed to date and the dollar amount remaining in the Contract to date.

The Contractor must send the original invoice to the Technical Authority's paying office [insert applicable Accounts Payable department] and one copy of the invoice to the Standing Offer Authority.

The original and copy of the invoice must be sent to the following location:
(Note to Offerors: this information will be completed at Standing Offer award.)

The Technical Authority's paying office [insert applicable Accounts Payable department] will send the invoices to the Technical Authority for approval and certification; the invoices will be returned to the paying office for all remaining certifications and payment action.

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

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

6.6 Limitation of Expenditure

Canada's total liability to the Contractor under the Contract must not exceed [insert $ amount]. Customs duties are included, and Applicable Taxes are extra.

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

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

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

(Note to Offerors: a finalized Resulting Contract Clauses section will be set out in the Final Challenge-Based Standing Offer Solicitation.)

Attachment A - Statement of Challenge

Problem Statement, Challenges, Minimum Viable Requirements and Personas

(Note to Bidders: a finalized Statement of Challenge, Attachments and Annexes will be set out in the Final Challenge-Based Solicitation.)

Problem Statement

Canada lacks an enterprise cloud-based security solution that provides the ability to deliver a consistent user experience from any device, any location, at any time.

In certain cases, Canada lacks cost-effective consistent security controls to protect GC data and assets to GC department remote sites and GC and Non-GC remote users, including SDAs (small department and agencies), when accessing the Internet, cloud-based SaaS, IaaS, and PaaS, and GC on-premise services. This results in lost productivity, high cost, lower user satisfaction and morale, increased cybersecurity risks, and inconsistent user experience.

Canada wishes to improve and optimize the ability to securely consume and deliver cloud-based services effectively, efficiently, and quickly.

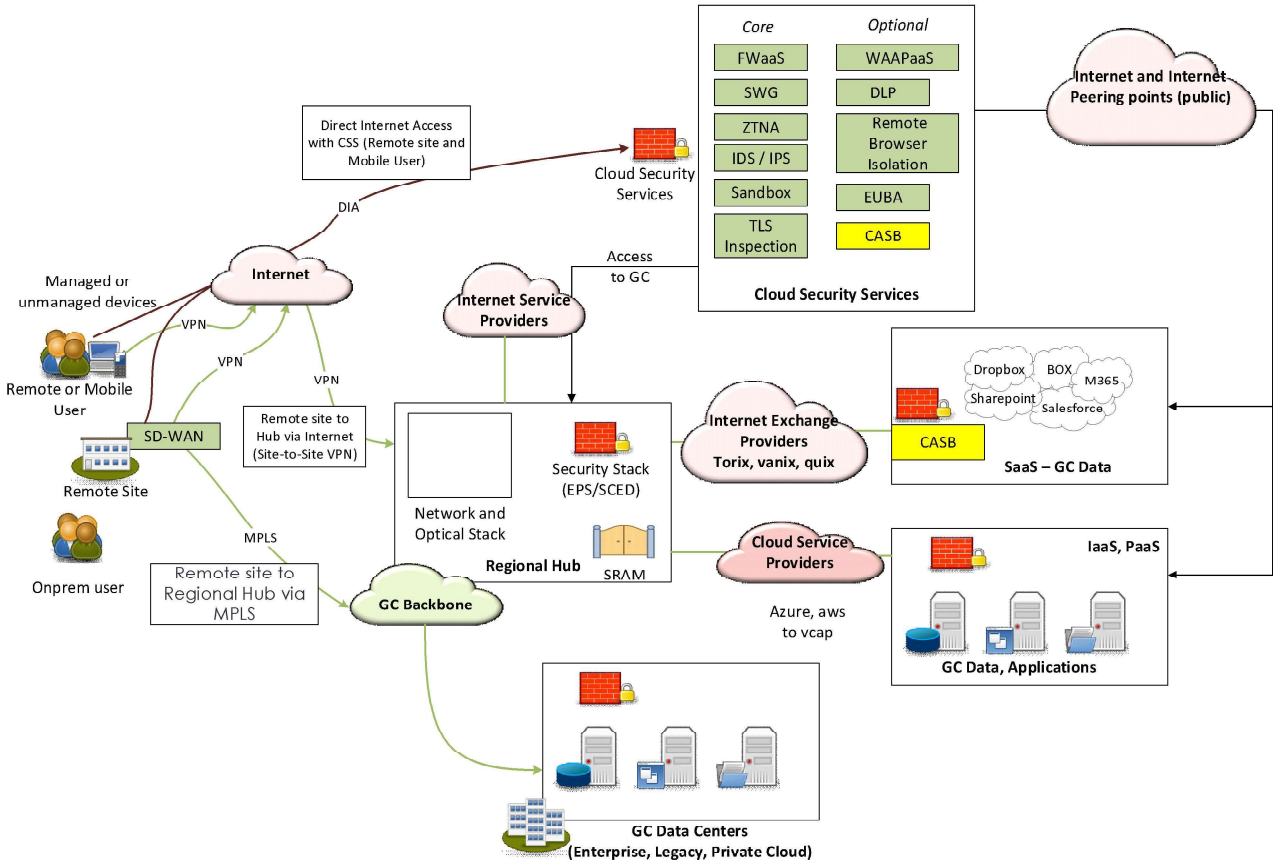
Challenges specific to the Solution

The problems to be solved by the Cloud Security Services can be summarized as follows:

- Inconsistent performance and user experience when accessing public cloud-based IaaS, SaaS and PaaS services.
- Using direct access to the Internet in order to access the public cloud or GC On-premise services exposes the GC and departments to threats. This includes users at remote sites, home offices, and mobile users. These “perimeters” must be protected appropriately.
- High costs associated with backhauling internet-bound traffic to regional GC hubs via MPLS circuits. Costs typically include the MPLS circuit, the cost of the internet circuits at EIS regional hub locations for that traffic, as well as the augmentation of the security stack at existing regional hubs. With respect to direct internet access, providing a GC-approved security stack at each remote location that has direct internet access is also costly.
- Inconsistent performance and user experience when accessing public cloud-based IaaS, SaaS and PaaS services.
- Inconsistent perimeter security services at remote locations, within some SSC partner departments, as well as within Small Departments and Agencies.

Proposed High-Level Architecture

The following proposed high-level architecture summarizes the previously mentioned use cases.



Uses cases based on Proposed High-Level Architecture

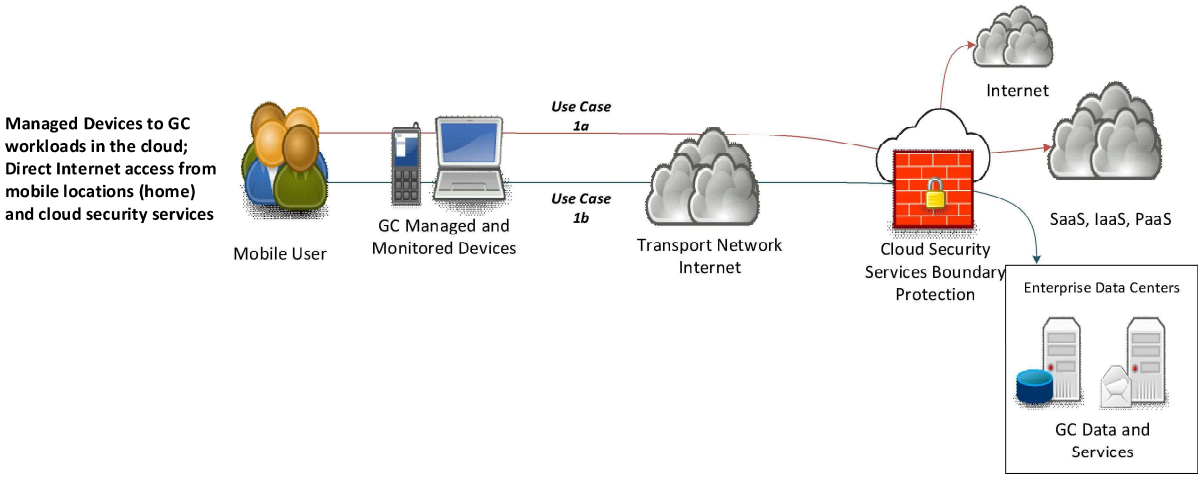
The following use cases constitute the operational environment in which SSC intends to take advantage of cloud security services.

1. Use Case 1a: Mobile User (managed device) accessing Cloud-Based Services

A GC mobile user with a managed device accesses cloud services, outside of a GC office (at home, hotel, public internet connection). All user traffic flows through a secure IPSec tunnel from the user's endpoint, to the CSS solution, then to the destination in the public cloud (general internet access, SaaS, IaaS, or PaaS).

Use Case 1b: Mobile User (managed device) accessing GC On-Prem (EDC) Services

A GC mobile user with a managed device accesses cloud services, outside of a GC office (at home, hotel, public internet connection, etc.), protected by security services within the CSS solution. All user traffic flows through a secure IPSec tunnel from the user's endpoint, to the CSS solution, then to the destination in a GC Enterprise Data Centre

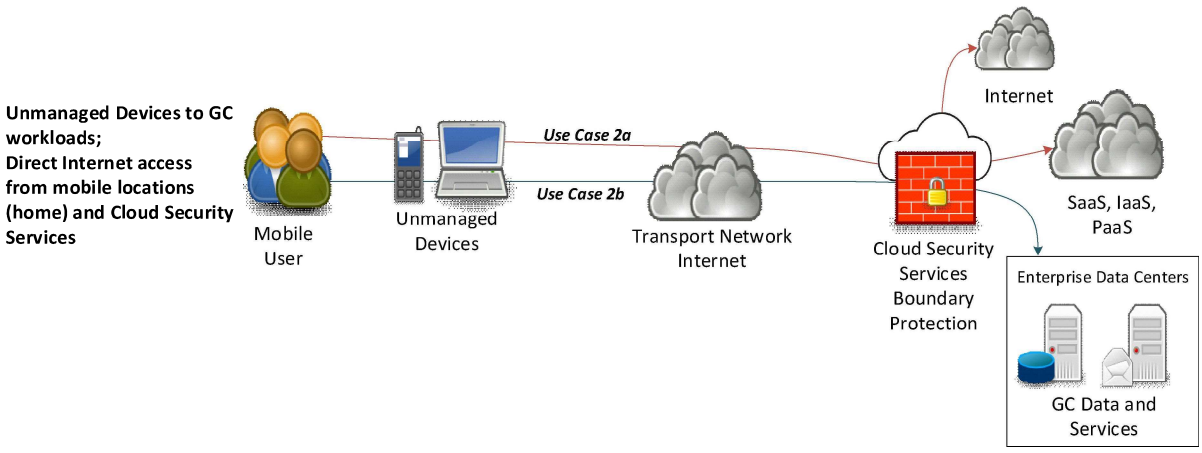


2. Use Case 2a: Mobile User (Unmanaged device) accessing Cloud-Based Services

A GC mobile user with a managed device accesses cloud services, outside of a GC office (at home, hotel, public internet connection). All user traffic flows through a secure IPSec tunnel from the user's endpoint, to the CSS solution, then to the destination in the public cloud (general internet access, SaaS, IaaS, or PaaS).

Use Case 2b: Mobile User (Unmanaged device) accessing GC On-Prem (EDC) Services

A GC mobile user with a managed device accesses cloud services, outside of a GC office (at home, hotel, public internet connection, etc.), protected by security services within the CSS solution. All user traffic flows through a secure IPSec tunnel from the user's endpoint, to the CSS solution, then to the destination in a GC Enterprise Data Centre.



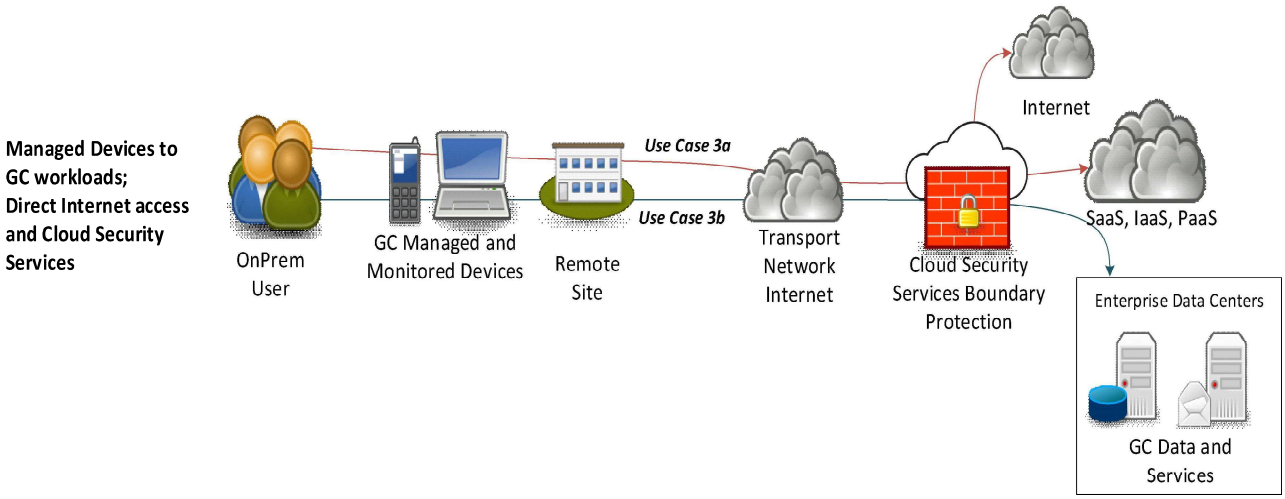
3. Use Case 3a: User (managed device) at a remote GC site accessing Cloud-Based Services

GC user with a managed device accesses cloud services a GC remote site's direct internet breakout, protected by security services within the CSS solution. Access to these services are based on the user's

profile, and optionally, the device's security posture. All user traffic flows through a secure IPSec tunnel to the CSS solution. Inbound traffic to the remote site's location is blocked, with certain exceptions as appropriate.

Use Case 3b: User (managed device) at a remote GC site accessing GC On-Prem (EDC) Services

GC user with a managed device accesses on-premise GC services located in a GC Enterprise Data Centre via a site's direct internet breakout, protected by security services within the CSS solution. Access to these services are based on the user's profile, and optionally, the device's security posture.

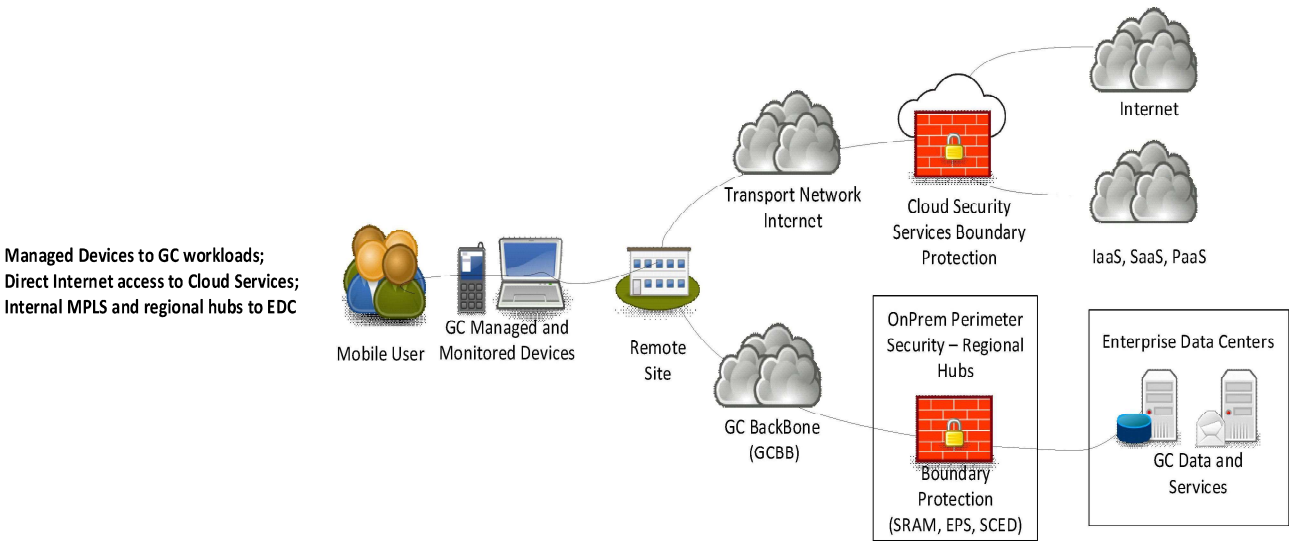


4. **Use Case 4: User with a managed device at a remote GC site accessing cloud-based services via the Internet, and GC On-Prem (EDC) Services via a Regional Hub.**

A user with a managed device at a remote building, accesses cloud-based services via a direct Internet connection. All user traffic flows through a security IPSec tunnel from the user to the CSS solution, then to the destination in the public cloud (general internet access, SaaS, IaaS).All traffic to and from the cloud-based services and the user flows through, and are protected by, the CSS solution.

Access to these cloud services are based on the user's profile, and optionally, the device's security posture. Traffic will be scanned for threats, may be blocked from going to known bad sites, etc. enhancing the security of the endpoint, reducing the treats to GC data and assets.

The user also accesses GC On-Prem (EDC) services via a GC Backbone (GCBB) MPLS circuit between the remote GC building and a regional hub. All traffic between the GC On-Prem (EDC) services and the user flows through the regional hub.



5. Use Case 5: Server-to-Server connections in a Multi-Cloud IaaS environment

A GC workload on a server in one IaaS environment (i.e. AWS, Azure, GCP) connects to another GC workload/server in a different IaaS environment, protected by security services within the CSS solution. Access to these services are based on policies.

Mandatory Minimum Viable Requirements

The sections below describe the expected minimum capabilities of the Solution. It describes:

- the functional requirements: what the solution must do (all the time) and must be able to do when prompted
- the non-functional requirement: how the solution must interact with the environment and other devices

Definitions

Able to – Expression that refers to a functionality or a component of the solution that must be actionable by users.

Multi-tenancy means that a single instance of the software and its supporting infrastructure may serve multiple customers. Each customer shares the software application and also shares a single database. Each tenant's data is isolated and remains invisible to other tenants.

Vendor refers to the Contractor that provides the solution under this contract.

1. Capabilities (CAP) :

CAP1: The solution must provide access to IaaS, PaaS, and SaaS cloud-based services to mobile users that:

a) use a GC managed device;
b) use an unmanaged device; and
c) are connecting via a direct internet connection

CAP2: The solution must provide secure access to any type of on-premise GC applications, data and services to mobile users that:

a) use a managed device;
b) use an unmanaged device; and
c) are connecting via a direct internet connection

CAP3: The solution must allow access to web-based and non-web-based applications and services, for managed and unmanaged devices, regardless of the location of the application and service, and location of the device.

CAP4: The solution must provide direct access to IaaS, PaaS, and SaaS cloud-based services to users located at GC remote sites that use a direct public internet connection, that:

a) use a managed device;
b) use an unmanaged device

CAP5: The solution must provide access to on-premise GC applications, data, and services to users located at GC remote sites that use a direct public internet connection, that:

a) use a managed device;
b) use an unmanaged device

CAP6: The solution must provide the following type of secure access between servers in a multi-cloud IaaS environment:

a) server-to-server communications between cloud IaaS providers, such as between AWS and Azure; and
b) Inter-region server-to-server communications, within a single cloud service provider, for example, between a server in Region 1, and a server in Region 2

CAP7: The solution must allow administrators to be able to configure user, group, and device access policies used to:

a) permit or deny user, group, and device access to services, regardless of where the service resides, based on access policies configured by the GC, and individual GC departments and agencies;

b) limit access to services, regardless of where the services reside, to those services that have been explicitly permitted, as defined within access policies created by the GC and individual GC departments and agencies;
c) deny any access and visibility to all services that a user, group, or device is not explicitly permitted to access.

2. Security (SEC):

SEC1: The solution must encrypt all data in transit while:

a) Enforcing secure connections to the Cloud Services, by providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;
b) Using up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CSE's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securelyconfiguring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-andprotected-b-information-itsp40111);
c) Using a minimum of 256-bit ECDSA key length;
d) Using a minimum of 2048-bit RSA key length.

SEC2: The solution must implement cryptographic protection using GC generated keys before any GC production data can be brokered through the solution.

SEC3: The solution must integrate the following federated identity methods:

a) Security Assertion Markup Language (SAML) 2.0 and OpenID Connect 1.0 where the End User credentials and authentication to cloud services are under the sole control of Canada; and
b) Microsoft ADFS integration via WS-FED.

3. Security Capabilities (SCAP):

SCAP1: The solution must provide protection against denial-of-service attacks (DDOS) on GC infrastructure.

SCAP2: The solution must limit user access to only the applications that they have been approved to access. Access to non-approved applications must be denied by the solution.

SCAP3: The solution must detect and act on suspicious user and device behaviour. For example, if suspicious user behaviour is detected, the solution must automatically deny access, quarantine the user or device, and report the suspicious behaviour to an administrator.

SCAP4: The solution must secure access to non web-based GC applications from a remote device that does not have a VPN client installed, on both managed Government Furnished Equipment (GFE) and unmanaged Bring Your Own Device (BYOD).

SCAP5: The solution must provide the following cloud-based perimeter security services:

a) Next Generation Firewall (NGFW);

b) Secure Web Gateway (SWG);
c) IDS/IPS;
d) Sandbox; and
e) TLS / SSL inspection.

SCAP6: The solution must track and log administrative changes. Changes must be audit logged with time, date, administrator username and change details.

SCAP7: The solution must transmit logs to the centralized GC SIEM, GC partner SOC/SIEM, and CCCS SOC systems.

SCAP8: The solution must be able to identify malware embedded in files in transit and files containing malware.

SCAP9: The solution's Secure Web Gateway component must recognize and be able to control web applications regardless of port and protocol.

SCAP10: The solution's Secure Web Gateway component must be able to identify the operating system and browser agent of the user, and trace activities back to individual users.

4. Authentication (AUTH):

AUTH1: The solution must be able to authenticate using the following GC authentication methods:

a) Authenticate devices using GC issued device certificates;
b) Perform LDAP, LDAPS, and OCSP authorization and authentication;
c) Authorize with LDAP group;
d) Authenticate and authorize with RADIUS;
e) Authenticate devices and users with SSO and SAML authentication mechanism;
f) Authenticate and Authorize with Open Authorization version 2 with OpenID (OAuth 2.0), or SAMLv2;

AUTH2: The solution must be able to use the following Multi-Factor Authentication (MFA) methods:

a) Multi-factor OTP device;
b) Soft token on portable device;
c) Multi-factor push notification to mobile device;
d) Government of Canada PKI user certificate;
e) Smart cards

AUTH3: The solution must be able to force users to use two-factor authentication (2FA).

5. Public Key Infrastructure (PKI):

PKI1: The solution must permit or deny access through the CSS solution based on the validity of GC certificates.

PKI3: The solution must display a message and deny connectivity if CRL server is unreachable

PKI4: The solution must provide inline decryption of SSL/TLS traffic using a root certificate provided by the GC.

6. Connectivity (CON):

CON1: The solution must peer with cloud service providers and internet exchange providers.

7. Interoperability (IOP):

IOP1: The solution must function on the following operating systems:

a) Microsoft supported Windows OS family;
b) Apple supported macOS and iOS family;
c) Google supported Android OS

8. Integration (INT):

INT1: The solution must integrate with GC SOAR solutions, using:

a) Representational State Transfer (REST);
b) Extensible Markup Language (XML).

INT2: The solution must function with a different vendor's CASB agent installed on an end-user's device. The solution's agent and the other vendor CASB agent must function together and direct traffic as defined by Canada.

INT3: The solution must integrate with Aruba Clear Pass and Cisco Identity Services Engine as the sources of zero trust policy engines.

INT4: The solution must apply the following Zero Trust approaches:

a) continuous evaluation and authorization of user identity and access requests,
b) enforcement of policy based on user profiles retrieved from one or more GC identity repositories
c) user and device identify based authorization, authentication, and access with contextual inputs (e.g., time of day, network location, user behaviour)

9. Management (MGMT):

MGMT1: Multi-Tenancy – The solution must allow multiple GC administrators from different organizations to manage, generate customized reports and administer specific portions of the solution within their authorized domain.

MGMT2: The solution must be able to apply Role-Based Access Control (RBAC) to users.

MGMT3: The solution must provide multi-tenant operator organizations through hierarchical RBAC in which the top-level organizations (Parent) have full visibility and control over all subordinate (Child) organizations and policies.

MGMT4: The solution must have the ability for the GC to implement global policies that apply to tenants, that cannot be changed or deleted by sub-tenants (Child) organization administrators.

MGMT4: The solution must restrict the ability of Child organizations to affect the policy or behavior of the solution for any other organization, including the Parent Organization.

MGMT5: The solution must be able to generate customized role-based ad-hoc reports.

10. Deployment and Operating Environment (ENV) :

ENV1: The solution must be able to be deployable in a High Availability (HA) configuration to ensure that device end-points are able to connect to the solution during an equipment or site failure.

ENV2: The solution must scale to a minimum of 100,000 concurrent users.

Personas

Persona Name

Dr. Abigail

Non GC users that need to access GC data (ie. educational institutions)

Demographics: Science

- Researcher at a university (could be an SME)
- Could be working on a masters or PhD or has a PhD

Goals • Scientists that need to access HPC to run algorithms • Easy and fast transfer of large quantities of data on and off the cluster – ie. Terabytes – the faster they are the more productive they will be • Easily access specific sites - Compute Canada or federated research data repository (FRDR) or other sites • Typically not real time traffic • Some could use streaming of traffic • Ability to have access on the fly (ie within 24 hours or less) • Provide access to and control of equipment (ie robots in the government labs) – still large amounts of data like high definition video or non-human / IoT/ Science devices (sensors streaming data in (automation needs to get data back into the facility to be analyzed)	**Challenges** • Some people using Linux environment – need to support multiple operating systems • Security tools – can reduce speed • Poor user experience, high latency • Security policies - How do we do identity management and how we do authentication • Users / scientists can't install software onto their computers • Not all types of access are at web browser or API driven • Access from outside Canada (global access requirement)
Values • Connection is simple (two factor authentication is sometimes pushed back on) • How they access will be similar to other systems they're familiar with	**Fears** • Extra hops – that may manipulate traffic and could slow it down • Fear of losing access - reliability and outages • Some research deals with sensitive data
Expectations • Once access is granted if performance is ok than they are ok • Once system is operational then how permissions are granted is done by researchers (within their department's control) – ie role based access and only permission will be given to which systems and whom (RBAC) • You get access to what you have access to and permissions to projects you have access to but not everything • 24 hour turn around – onboarding and offboarding collaborators • Look and feel is similar to what they're used to • Need High Availability • Ticketing system to support external users – support model for scientists for quick resolution (ITSM)	**Measures of Success** 1. Have fast and flexible connectivity for moving data (speed) 2. User experience – as seamless and with as few steps as possible 3. User logs once and they go through to what they need to access (only login once) – simplicity of use • Without installing new software • Failover

Persona Name

Penelope

ISO/SOC

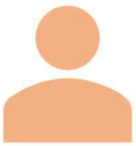
Demographics:

- CS2 to CS4 both ISO and SOC

Goals • Ensure love and care of technology and infrastructure of the cloud solutions is taken care of • Incident response – augment incident response capabilities • Access management (ensure the right people have the right privileges)	**Challenges** • Staff to manage solution • Data quality – not getting adequate logging data • Data volume – data increases and collision of data if its not tagged properly • Getting the right people to do the work – hard to get SOC bilingual people – reskilling resources and training
Values • Having better visibility • Dealing with the disparate internet connections (not being monitored / insecure) • Better security	**Fears** • Would be duplicating other services that may be able to provide a different flavour of solution comparable to CSS • By multiple options it creates more complexity and therefore more risk is introduced • How can we guarantee integrity of the services (so that they haven't been tampered with) – we don't manage the security control and how it will change over time and vulnerability management • Partners go around SSC to take control of their domain – will there be guard rails in place to prevent mistakes
Expectations • Would be nice to have a centralized place to manage tenants – to be able to access all tenants, like cyber events – if something needs to be replaced everywhere how fast can we reach them? (SSC, CRA, etc tenants) - Centralized cartography – observability • Global policy may impact every partner and specific policy for departments (parent/child multitenancy) • Integration with other security services for monitoring, observability, visibility • Pre-massage and prepare data to help with data quality and volume issues (so when data is corelated it makes sense) • Maintain / track source IP address • Ability to copy or apply settings to all tenants • Well architected RACI if this is a federated model – accountability of change needs to be in place • Solid change management (from baseline of global policy) • Availability of 99.999 and 7/24 • A way to monitor health of environment – or access to staff that can help issues like performance and reliability	**Measures of Success** 1. Have observability of entire infrastructure 2. Useful information – integration, easily available - actionable telemetry (not creating more work) – solution tells us where to look 3. Reduced effort to triage incidents 4. Increase security posture – ie. split tunneling may expose some part of the infrastructure – ie. when traffic not through VPN • Preserve log data *(integrity of logs, all logs are sent, and logs aren't lost)* • Properly architected – RBAC inclusion of two factor authentication • Ease of use – GUI and no need to engage professional services, no need to script • Global application of tenancy • Meet language and accessibility requirements

Persona Name - Sierra

Department and SDA tenant admins



Demographics:

- RE5 to 6, CS4

Goals • Access to logs end to end – real time sharing of information (to mitigate incident) including SSC portions • IoT (non-human devices) – ie. camera with a 4G card uploading – any time, any place and any device – we want to protect and authenticate these devices • Integrating with partners, AD and PKI • Ease of use	**Challenges** • With security events, if some are managed by SSC it is hard to see and identify what has happened • What is in place for data residencies (does data stay in Canada?) • Decrypting data • Having enhanced reliability for data • TD5 threat profile – have additional security measures
Values	**Fears** • Poor performance (user experience) • Without clear RACI – there could be finger pointing – have everyone accountable for their portions (internal to government)
Expectations • Integration with existing security controls - Perimeter security infrastructure would work with CSS • Flexibility to be able to tailor based on department needs – every department gets its own tenancy • Departmental admins would manage the department (ie. department maintains their own) • Global policy across all tenants • KPIs and reporting – executive reports – to showcase the security level to partners based on evidence and prove the information is secure, trends – to have their minds at ease that incidents were responded to quickly • For those with minimal IT teams, have more automation or machine learning to reduce management of system – as much as possible	**Measures of Success** 1. Make us more secure 2. Automated action to mitigate the impact of incident 3. User experience – end user doesn't know it exists; they can just connect to what they need to connect to – don't need to worry about complexity of the network infrastructure • AI for unforeseen intrusion and malware • Uptime – no downtime • No latency – speed of accessing information from end user perspective • From operational /admin perspective have automated – no additional resources – don't want another system to support with same number of resources

Persona Name - Isabelle

GC Employees / Contractors – accessing remotely

Demographics:

- Everyone working remotely full time
- Located across Canada
- Significant increased use of cloud based services – due to remotely working and Government of Canada increasing cloud based services
- Accessing collaboration tools, office tools, corporate tools and government specific corporate and office tools
- Departmental specific applications on premises and in the cloud
- Accessing internal Government of Canada applications and cloud based
- Accessing mostly 9 am to 5 pm in their time zone

Goals • Accessing applications (and do it quickly) • Have application responsiveness (not wait 20 seconds after click) • Not have to go through unnecessary steps (ie no additional verification) • Common look and feel – do it the same way they do it in the office • Do our work and accomplish tasks without network/connectivity in the way – transparent/invisible • Privacy and confidentiality	**Challenges** • Capacity (of applications and network) to handle remote work • Can't have 12 people with their video turned on • Performance when accessing applications and their responsiveness (not as fast as in the office) • Particular application access may be difficult (ie. ESDC and others with more self-imposed policies)
Values • Privacy and security as an employee are maintained • Being able to do their job • Speed / responsiveness of applications that need to be access • Productivity (and ability to do job)	**Fears** • Congestion (too many people trying to get on the network at the same time) • Waking up to another lockdown – with a kids and everyone on the network at the same time,…. • Technical issues while working remotely, new solution or new process they have to follow (can't turn to person next to me for help or have someone come and help – and if it impacts collaboration tools, can't ask for anyone's help – leads to isolation) • Losing our work (networked applications don't save, network timeout, things crash) • Losing productivity and not being able to access what they need (and missing timelines)
Expectations • Single sign on • Remote access solution actually works • Invisible – connecting easily without many steps • Connecting on any device we have (ie things like email, Teams,…) • Support when it breaks (it just doesn't work, and don't know why) • More rapid adoption of new services • Quick internet browsing / access	**Measures of Success** 1. Quick response from applications being accessed 2. No disconnects / interruptions in the service 3. Ease of use – don't avoid using it – don't hate the service • Access what is needed, when it is needed • Low number of issues • Connection is simple and few (or one) steps

Attachment A1 - Cloud Security Requirements

Cloud Security Requirements

(Note to Offerors: in addition to the security requirements outlined in the section entitled *Security Requirements*, (CBSOS 1.9), a finalized Attachment A1 – Cloud Security Requirements will be set out in the Final Challenge-Based Standing Offer Solicitation.)

Cloud Tiering Assurance Model

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

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

Government of Canada - Cloud Tiering Assurance Model

Requirements	Tier 0	Tier 1	Tier 2	Tier 3
GC Impact	Very Low	Low	Moderate	High
Categorization	Unclassified	Up to and including Protected A, Low Integrity, Low Availability	Up to and including Protected B, Medium Integrity, Medium Availability	Above Protected B
Data Residency	Anywhere	Anywhere	In Canada	In Canada
Location	Off-premise	Off-premise	Off-premise	On premise
Deployment Model	Public	Private, Public, Community, Hybrid	Private, Public, Community, Hybrid	Private, Community
Service Model	SaaS	IaaS, PaaS, SaaS	IaaS, PaaS, SaaS	Not applicable
Compliance *Application* *Platform* *Resource Abstraction Layer,* *Hardware, Facilities*	Self-assessment to CSA Cloud Controls Matrix OR ISO 27001 OR SOC 2 Type II OR Departmental Assessment	Inherited from GC-approved Cloud Service Provider **OR** ISO 27001 OR SOC 2 Type II AND Self-assessment to CSA Cloud Controls Matrix	IInherited from GC-approved Cloud Service Provider **OR** ISO 27001 AND ISO 27017 AND SOC 2 Type II for the trust principles of security, availability, processing integrity, and confidentiality	Not applicable
Privacy	Not applicable	Privacy Controls Attestation (TBD)	ISO 27018	Not applicable

Certifications

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

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

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

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

Cloud Service Provider (CSP) IT Security Assessment Program

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

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

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

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

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