REQUEST FOR PROPOSALS (RFP)
FOR
CONFERENCING AND OPERATOR ASSISTED SERVICES
on behalf of SHARED SERVICES CANADA

Request for Proposals (RFP): BPM xxxx

Date of issuance: 2023-XX-XX

Request for Proposals (RFP) for Conferencing and Operator Assisted Services on behalf of Shared Services Canada (SSC)

P2P Soliciation No.	P2P 105809	**Date of Issuance**	2023-xx-xx
Client Reference No.	xxx	**Requisition No.**	xx

THIS DOCUMENT CONTAINS A SECURITY REQUIREMENT.

Issuing Office	**Shared Services Canada**	
Contracting Authority **(The Contracting Authority is the contact for all questions and comments about this document)**	**Name**	Eric Vanasse
	Telephone No.	514-607-8519
	Email Address	Eric.Vanasse@ssc-spc.gc.ca
	Postal Address	400 Cooper Street Ottawa, Ontario K2P 2N1
Closing Date and Time ("Solicitation Closing")	xx days from posting date, 2pm	
Time Zone	Eastern Time (ET) Ottawa, Ontario, Canada	
Destination of Goods/Services	Destinations within Canada TBD for Each Requirement	
Email Address for Bid Submission by the Closing Date and Time	xx	

TABLE OF CONTENTS

Contents

List of Annexes to the Resulting Contract:

Annex A	Statement of Work - General
Annex B	Statement of Work – Audio/Web
Annex C	Statement of Work – Operator Assisted Services
Annex D	Security Requirements Check List Pricing Sheet
Annex E	Pricing Sheet (at contract award)
Annex F	COAS CSP Security Obligations
Annex G	SCSI Submission Form
Annex X	Federal Contractors Program for Employment Equity – Certification (TBD)
Annex X	Insurance Requirements (TBD)

List of Attachments to Part 1 (General Information):
- Attachment 1.1: Standard Instructions for Procurement Documents, Version 1.4

List of Attachments to Part 2 (Bidder Instructions):
- Attachment 2.1: XXX

List of Attachments to Part 3 (Bid Preparation Instructions):
- Attachment 3.1: XXX

List of Attachments to Part 4 (Evaluation Procedures and Basis of Selection):
- Attachment 4.1: Technical Evaluation
- Attachment 4.2: Financial Evaluation (Annex E – Pricing Table at contract award)

List of Attachments to Part 5 (Certifications):
- Attachment 5.1: XXX

List of Attachments to Part 6 (Security, Financial and Other Requirements):
- Attachment 6.1: XXX

Forms:

- Form 1 - Bid Submission Form (incl in draft RFP)
- Form 2 – Integrity Form (TBD)
- Form 3 - Substantiation of Technical Compliance Form (TBD)

- Form 4 - OEM Certification Form (TBD)
- Form 5 - Software Publisher Certification Form (TBD)
- Form 6 - Software Publisher Authorization Form (TBD)
- Form 7 – Socio-Economic Report Form (TBD)

PART 1 GENERAL INFORMATION

1.1 Introduction

The bid solicitation is divided into seven parts plus attachments, forms and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, if applicable, and the basis of selection; and

Part 5 Certifications: includes the certifications to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The annexes include the Statement of Work and any other annexes.

1.2 Summary

1.2.1 **Nature of the Requirement:** Shared Services Canada (SSC) has a requirement for the provision of Conferencing and Operator Assisted Conferencing Services (COAS) (the "**COAS Services**") as further described in section 1.2.4 below.

1.2.2 Audio/Web Conferencing Services (the "**AWCS**") are required for collaborative conferences, meetings, large group events and are hosted on a cloud-based Software as a Service (SaaS) application platform, whereas the Operator Assisted Service (the "**OAS**") are required for virtual events, briefings, press conferences and meetings where operator resources are required to manage and monitor the conference when scheduled, as-and-when required.

1.2.3 The COAS Service must be compliant with the Government of Canada's Official Languages Act, the Accessible Canada Act, and the security requirements as specified in the contract.

1.2.4 The scope of the COAS Services is as follows:

1.2.4.1 An outsourced, modern, accessible, and reliable AWCS, as further specified in Annex B – Audio/Web Conferencing SOW, using an application platform accessible to users over the Internet that allows conference Hosts, Co-Hosts and Participants to connect via:

1.2.4.1.1 A telephone (mobile or landline);

1.2.4.1.2 A browser-based web client that supports audio, video and content sharing capabilities; and

1.2.4.1.3 A Standards-Based (SIP) Videoconferencing Endpoint;

1.2.4.2 The OAS is available to GC users for pre-conferencing, in-conferencing and post-conference support with their conference as further specified in Annex C – Operator Assisted Services SOW;

1.2.4.3 A Service Portal accessible by a browser that allows account management, conference scheduling, reporting and service management for all COAS Services.

1.2.5 **Potential Client Users:**

1.2.5.1 "**Client**" means SSC and its Partner Departments, and Other Government Departments

1.2.5.2 "**Partner Department**" or "**Partners**" mean those government institutions for which SSC's services are mandatory as specified by an Order In Council and includes SSC itself.

1.2.5.3 "Other Government **Departments**" or "**Government Departments**" means a user of the COAS Services that is not a Partner Department or a Partner.

1.2.5.4 This solicitation is being issued by SSC. It is intended that the contract resulting from this solicitation will be used by SSC to provide shared services to Clients, Partners and Other Government Departments

1.2.6 **Number of Contracts**: SSC intends to award one (1) contract to the successful bidder. This bid solicitation does not preclude Canada from using another method of supply for entities of the Government of Canada with the same or similar needs.

1.2.7 **Term of Contract**: SSC intends to award a contract for a contract period of 4 years, plus 6 one-year irrevocable options allowing Canada to extend the term of the contract.

1.2.8 **Re-Tender if No Compliant Bids Received**: If no compliant bids are received, Canada reserves the right to re-tender the bid solicitation, with or without changes by posting on Buy and Sell.

1.3 Security Requirements:

1.3.1 There are security requirements associated with this requirement. For additional information, see Part 7 – Resulting Contract Clauses.

1.3.2 Canada will require the top 3 ranked responsive bidders, as determined by Canada following bid evaluation, to comply with the Supply Chain Integrity (SCI) Assessment and the Cloud Service Provider Information Technology Security (CSP ITS) Assessment specified below. Of these Bidders, only the top-ranked Bidder will be requested to comply with the Contract Security Program. If the top-ranked Bidder does not meet both the SCI Assessment and the CSP ITS Assessment, then the second-ranked Bidder will be requested to comply with the Contract Security Program. If the second-ranked Bidder does not comply with the Contract Security Program, then the third-ranked Bidder will be requested to comply with the Contract Security Program. If none of these Bidders meet these requirements, then Canada may, but will have no obligation to, continue down the list of responsive Bidders until one responsive Bidder meets each of the Contract Security Program, the SCI Assessment and the CSP ITS Assessment. A responsive Bidder must meet all the security requirements specified in section 1.3 to be eligible for contract award.

1.3.3 **Contract Security Program:** The Contract Security Program will apply as specified in section 1.3.2. For additional information, consult Annex D – Security Requirements Check List (SRCL).

1.3.3.1 For more information on personnel and organization security screening or security clauses, Bidders should refer to the Contract Security Program of Public Services and Procurement Canada (PSPC) Security requirements for contracting with the Government of Canada – Canada.ca (tpsgc-pwgsc.gc.ca)website.

1.3.3.2 All personnel assigned to provide services must have a current security clearance to the level specified in any Contract against this RFP, granted by the PSPC Canadian Industrial Security Directorate.

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

1.3.4.1 The Supply Chain Integrity (SCI) Assessment will apply as specified in section 1.3.2. Responsive Bidders must provide the information specified at **Annex G – Supply Chain Security Information (SCSI)** to Canada upon request. SCI is an important corporate requirement. Challenged by an increasingly complex cyber threat environment, Canada is committed to applying enhanced security process and contract clauses to the acquisition of both products and services. The purpose of the SCI Assessment is to ensure that all proposed sub-contractors, products, equipment, software, firmware and services that are procured by SSC meet the required security and supply chain standards as determined by Canada.

1.3.4.2 Canada will assess information submitted by the Bidder in accordance with **Annex G – Supply Chain Security Information**. The Bidder must achieve an SCSI at a risk level of medium or lower in order for the bid to be declared responsive. An SCI Assessment that is compliant with the risk level above will not alter the Bidder's ranking. This means that if the top-ranked Bidder achieves a "medium" SCI Assessment and the second-ranked Bidder achieves a "low" SCI Assessment, the ranking for each respective Bidder remains unchanged.

1.3.5 **Cloud Service Provider Information Technology Security (CSP ITS) Assessment:**

1.3.5.1 The CSP ITS Assessment will apply as specified in section 1.3.2. Responsive bidders must undergo a CPS ITS Assessment upon request by Canada. The CSP Assessment is an important corporate requirement. The Bidder's Cloud Service Provider's security capabilities and deficiencies must include ITS, the physical security of the CSP's data centres, the personnel security of its privileged users, its adherence to Canadian privacy regulations, as well as other areas.

1.3.5.2 The purpose of this program is for the GC to determine that the ITS capabilities and residual risks for the cloud service being used by the GC is satisfied to an acceptable level for the requirements of the GC-selected security controls and enhancements as outlined in *ITSG-33 IT Security Risk Management: A Lifecycle Approach*.

1.3.5.3 Canada will assess the CSP ITS information submitted by the Bidder in accordance with **Annex F**. Canada must approve the CSP ITS Assessment at a risk level of medium or lower in order for the bid to be declared responsive. A CSP ITS Assessment that is compliant with the risk level above will not alter the Bidder's ranking. This means that if the top-ranked Bidder achieves a "medium" CSP ITS Assessment and the second-ranked Bidder achieves a "low" CSP ITS Assessment, the ranking for each respective Bidder remains

unchanged. For greater clarity, if the Bidder's Cloud Service Provider does not meet the CSP ITS Assessment requirement at the "medium" or lower risk level, the Bidder will be declared non-responsive.

1.3.6 **Trade Agreements:**

The following trade agreements apply to this procurement process:

Trade Agreements	**Yes/No**
Canadian Free Trade Agreement	Yes
Canada-Korea Free Trade Agreement	Yes
World Trade Organization Agreement on Government Procurement	Yes
Canada-Chile Free Trade Agreement	Yes
Canada-Colombia Free Trade Agreement	Yes
Canada-Peru Free Trade Agreement	Yes
Canada-Panama Free Trade Agreement	Yes
Canada-Honduras Free Trade Agreement	Yes
Canada-Ukraine Free Trade Agreement	Yes
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	Yes
Canada-European Union Comprehensive Economic and Trade Agreement (CETA)	Yes

1.4 **Conflict of Interest or Unfair Advantage**

1.4.1 As set out in SSC's Standard Instructions for Procurement, Version 1.4, a bid can be rejected due to an actual or apparent conflict of interest or unfair advantage.

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

1.4.2.1 Canada has used the services of private sector consultants and subcontractors of the following firms in preparing strategies and documentation related to this COAS Procurement Process:

1.4.2.1.1 Ibiska: Colin Bush, Yvonne Robinson

1.4.2.1.2 Maplesoft Consulting Inc.: Ripu Rishi

1.4.2.1.3 Protak Consulting Group Inc.: Todd Hutchins

1.4.2.1.4 Calian: Lyne Cousineau

1.4.2.1.5 Glencastle Security Inc. (GSI): Elizabeth Wolkowycki, Robert Coulas

1.4.2.1.6 MDOS Consulting; Geordie Davis

1.4.2.1.7 Maxsys: Rob McClure

1.4.2.2 The persons identified in the above paragraph, and their respective directors, officers, partners, subcontractors, employees, and affiliates (as defined in the Canada Business Corporations Act R.S.C.1985 c. C-44), including current directors, officers, partners and employees and any of the foregoing who leave that employment or engagement ("Restricted Parties") are:

1.4.2.2.1 Not eligible to participate as a Bidder to this RFP or as a Bidder to any subsequent solicitations related to the COAS Procurement Process;

1.4.2.2.2 Prohibited from providing advice to any Bidder, directly or indirectly, with respect to the preparation of a bid or the negotiation of any subsequent contract related to the COAS Procurement Process; and

1.4.2.2.3 Prohibited from participating in the negotiation of any subsequent contract related to this RFP in any way as an employee, advisor, consultant, subcontractor, or otherwise in connection with any Bidder.

1.4.2.3 No Bidder will consult, include, or seek advice from any Restricted Party in connection with a bid to this RFP nor in the finalization of any contract awarded thereafter.

1.4.2.4 Any bid in violation of any of the provisions of this Section 1.5 will be deemed to be in real or perceived conflict of interest and will be considered non-responsive. If a violation is discovered after award of any contract, the violation shall be grounds for termination of the contract under the default provisions of the contract.

1.4.2.5 By submitting a bid, the Bidder represents and warrants that the bid was prepared in accordance with section **Error! Reference source not found.**5 – Conflict of Interest and Unfair Advantage.

1.5 Phases of the COAS Procurement Process

1.5.1 Following the COAS Buy and Sell posting and subsequent communications, the remaining phases of the COAS Procurement Process as identified below which starts with the Draft Request for Proposals (Draft RFP) and moves to the implementation of the COAS in the following order:

1.5.1.1 **Draft Request for Proposals (RFP):** Draft RFP includes details of the requirement in the Statements of Work (SOW) for the Services in both of Canada's official languages and is intended to solicit industry feedback. Draft RFP provided is being sent for industry feedback, including opportunity for a one-on-one meeting, if requested.

1.5.1.2 **Request for Proposals (RFP) Phase:** This RFP provides details of the requirement for the Services in both of Canada's official languages including mandatory requirements. All bids submitted by Solicitation Closing will be evaluated in accordance with the requirements set out in the RFP.

1.5.1.3 **Contract Award:** Canada anticipates awarding one (1) contract to one (1) Contractor for the requirements.

1.5.1.4 **Operational Readiness Phase**: as described in Annex A: General SOW

1.5.1.4.1 **SA&A In-Service:** Following assessment by SSC of the security requirements for SA&A, SSC will issue an Authorization to Operate (ATO) in writing for the COAS.

1.5.1.5 **Operations Phase:** as described in Annex A; General SOW

1.5.1.5.1 Issuance of Service Requests and Reservations: Service Requests and Reservations are issued to provide COAS services:

1.6 Shared Services Canada's Role in Promoting Accessibility

1.6.1 The Accessible *Canada Act* is intended to enhance the full and equal participation of all persons, especially persons with disabilities, in society. This is to be achieved through the progressive realization, under federal jurisdiction, of a Canada without barriers, particularly by the identification, removal and prevention of barriers.

1.6.2 SSC has a role in implementing the Government of Canada's (GC) vision for a more accessible Canada because SSC provides the information technology infrastructure that supports the delivery of digital services to Canadians and GC employees. This means that SSC is engaged in the procurement of goods and services and in supporting the delivery of programs and services by other government departments, both of which are areas covered by the *Accessible Canada Act*. SSC's goal is for its information technology infrastructure to be more accessible to and more usable by the broadest range of government officials and Canadians who use it, including those with disabilities.

1.6.3 SSC is committed to providing leadership to procure accessible Information Communication Technology (ICT) goods and services and supporting the goal of "inclusive by design, accessible by default". Future stages of the procurement process may include accessibility requirements which are adopted from the EN 301 549 (2018) Harmonized European Standard Accessibility Requirements for ICT Products and Services.

1.6.4 As the intention is for the Project to take place progressively, suppliers should anticipate that, over time, the accessibility requirements in Canada's procurement contracts will evolve and may become more comprehensive.

1.7 Canada's Policy on Green Procurement:

1.7.1 In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process Policy on Green Procurement (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32573). To assist Canada in reaching its objectives, bidders should:

1.7.1.1 Include all environmental certification(s) relevant to your organization (e.g., ISO 14001, Leadership in Energy and Environmental Design (LEED), Carbon Disclosure Project, etc.)

1.7.1.2 Include all environmental certification(s) or Environmental Product Declaration(s) (EPD) specific to your product/service (e.g., Forest Stewardship Council (FSC), ENERGYSTAR, etc.)

1.8 Shared Services Canada's Role in Promoting Socio-Economic Benefits

1.8.1 SSC encourages bidders to subcontract with small and medium enterprises, as well as suppliers from underrepresented groups. More information is available in Form xx – Socio-Economic Report Form.

1.9 Debriefings

1.9.1 Unsuccessful Bidders may request a debriefing on the results of the bid solicitation process. Unsuccessful Bidders should make the request to the Contracting Authority within 15 Federal Government workdays of receipt of the results of the RFP. The debriefing may be provided in writing, by telephone or virtually at Canada's discretion.

PART 2 BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

2.1.1 All instructions, clauses and conditions identified in this document or any of its attachments by number, date and title are:

2.1.1.1 As set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

2.1.1.2 These documents are incorporated by reference and they form part of this document as though they were expressly set out here in full.

2.1.2 SSC's Standard Instruction for Procurement Documents No. 1.4 ("**SSC's Standard Instructions**") are incorporated by reference into and form part of the solicitation. If there is a conflict between the provisions of SSC's Standard Instructions and this document, this document prevails. SSC's Standard Instructions are provided with this bid solicitation.

2.1.3 With respect to SSC's Standard Instructions:

2.1.3.1 There will be a demonstration by the top-ranked Bidder with respect to this bid solicitation.

2.1.3.2 Instead of the bid validity period set out in SSC's Standard Instructions, the bid validity period will be 360 days.

2.1.4 By submitting a bid, the Bidder is confirming that it agrees to be bound by all the instructions, clauses and conditions of the solicitation.

2.1.5 The 2003-1 Supplemental Standard Instructions - Telecommunications _2015-04-01 are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003-1 and this document, this document prevails.

2.2 Submission of Only One Bid:

2.2.1 For the purposes of this article, "**Related Entities**" means all entities (whether those entities include one or more natural persons, corporations, partnerships, limited liability partnerships, etc.) that are related to one another. Regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law, entities are considered "**related**" for the purposes of this RFP if:

2.2.1.1 they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);

2.2.1.2 they are "related persons" or "affiliated persons" according to the *Canada Income Tax Act*;

2.2.1.3 the entities have now or in the two years before Solicitation Closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

2.2.1.4 the ` otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

2.2.2 Each Bidder will be permitted to qualify only once. If a Bidder or any Related Entities participate in more than one bid (participating means being the, or part of the Bidder, including any member of the Joint Venture that comprises the Bidder identified on more than on Bid Submission Form). Canada may, in its sole discretion disqualify all such Bidders or provide those Bidders with two FGWDs to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all bids from members of the related group being declared non-responsive and disqualified.

2.2.3 By submitting a bid, the Bidder certifies that it does not consider itself to be a Related Entity to any other Bidder. For greater clarity, where a Cloud Service Provider is not a member of a Joint Venture submitting a bid to this RFP, that Cloud Service Provider may be proposed by any Bidder as a subcontractor. This means that Cloud Service Provider "L" that is not a joint venture member of any Bidder to this RFP could be proposed as a subcontractor by Bidder "M", Bidder "N" and Bidder "O".

2.2.4 (please see Article 2.6.4 regarding relying on the experience of corporate predecessors or proposed subcontractors)

2.2.5 In the case of a joint venture Bid, each COAS Mandatory Technical Requirement Experience can be met by a different joint venture member. The Service Project References are not required to be projects performed by both the entities of the joint venture itself.

2.2.6 Canada will only consider the experience of the Bidder, or in the case of a joint venture, the joint venture member itself (not including any affiliate of the Bidder), subject to the following:

2.2.6.1 The experience of a corporate predecessor will be evaluated as experience of the Bidder, if:

2.2.6.1.1 The corporate predecessor amalgamated with another corporation to form the Bid; or

2.2.6.1.2 All or substantially all the assets of the corporate predecessor were acquired by the Bidder, the majority of the corporate predecessor employees became employees of the Bidder, and both the corporate predecessor and the Bidder carry on essentially the same business; or

2.2.6.1.3 All or substantially all of a specific business unit that was responsible within the corporate predecessor for the work connected with the experience requirement has been transferred to the Bidder, along with all or substantially all the employees of that business unit, and the Bidder continues to carry on essentially the same business as that business unit.

2.2.6.2 For those requirements specifically identified in Annexes A, B, and C as allowing a Bidder to qualify based on the previous experience of a proposed subcontractor, Canada will consider the experience of subcontractors for qualification purposes. For proposed subcontractors' experience, the Bidder must provide all the same required information demonstrating the experience and indicate that the experience is that of a proposed subcontractor. However, for any Bidder that relies on the experience of a proposed subcontractor, the Bidder will be required, at the RFP and during the performance of any resulting contract, to continue to provide the services of that subcontractor, unless the consent of the Contracting Authority is given to make a change. Although a Bidder may rely on the experience of a subcontractor as set out in Annexes A, B, and C, no subcontractor will be permitted to participate in the RFP.

2.3 Electronic Submission of Bids

2.3.1 **Email Submission of Bids:** Bidders must submit their responses by email in accordance with this section by the Solicitation Closing to the email address identified on the cover page of this document as the "Email Address for Bid Submission" **Email Title:** Bidders are requested to include the Solicitation No. identified on the cover page of this document in the "subject" line of each email forming part of the bid.

2.3.2 **Email Size:** Bidders should ensure that they submit their bid in multiple emails if any single email, including attachments, will exceed 15 MB.

2.3.3 **Time of Receipt:** All emails received at the Email Address for Bid Submission showing a "received" time before Solicitation Closing will be considered timely. In the case of a dispute regarding the time at which an email arrived at SSC, the time at which the bid is received by SSC will be determined:

2.3.3.1 by the delivery time stamp received by the Bidder if the Bidder has turned on Delivery Status Notification for the sent email in accordance with RFC 1891 established by the Internet Engineering Steering Group (SMTP Service Extension for Delivery Status Notification); or

2.3.3.2 in accordance with the date and time stamp on the SMTP headers showing the time of first arrival on a server used to provide the Government of Canada with email services, if the Bidder has not turned on Delivery Status Notification for the sent email.

2.3.4 **Email Acknowledgement of Receipt by SSC:** On the closing date, an SSC representative will send an email acknowledging receipt of each bid (and each email forming part of that bid, if multiple emails are received) that was received by Solicitation Closing.

2.3.5 **Responsibility for Technical Problems:** By submitting a bid, the Bidder is confirming that it agrees that Canada is not responsible for:

2.3.5.1 any technical problems experienced by the Bidder in submitting its bid, including attachments rejected or quarantined because they contain malware or other code that is screened out by SSC for security reasons; or

2.3.5.2 any technical problems that prevent SSC from opening the attachments. For example, if an attachment is corrupted or otherwise cannot be opened or cannot be read, it will be evaluated without that portion of the bid. Bidders will not be permitted to submit substitute attachments to replace any that are corrupt or empty or submitted in an format other than those specified in section 3.2.10 **Format of Bids**.

2.3.6 **Alternate Email Address for Bid Submission:** Where the Bidder is having technical difficulties with the Email Address for Bid Submission that are caused by SSC, SSC will accept email-delivered bids at [insert alternate email address] (the "Alternate Email Address for Bid Submission"). Where a Bidder submits bids through both the Email Address for Bid Submission and the Alternate Email Address for Bid Submission, the bid with the earlier time stamp will be evaluated by SSC. After Solicitation Closing, bids delivered to either the Email Address for Bid Submission or the Alternate Email Address for Bid Submission are no longer admissible and will not be evaluated or considered by SSC.

2.3.7 **Format of Bids:** Unless specified otherwise in the RFP, Bidders must submit documents in either of the following formats:

2.3.7.1 PDF attachments; or

2.3.7.2 documents that can be viewed using either Microsoft Word or Microsoft Excel.

Note: Bidders that submit documents in other formats will be deemed non-responsive.

2.3.8 **Availability of Contract Authority:** During the four (4) hours leading up to Solicitation Closing, an SSC representative will monitor the Email Address for Bid Submission and the Alternate Email Address for Bid Submission and will be available by telephone at the Contracting Authority's telephone number shown on the cover page of this document (although the SSC representative may not be the Contracting Authority). If the Bidder is experiencing difficulties transmitting the email to the email address, the Bidder should contact SSC immediately at the Contracting Authority's coordinates provided on the cover page of this document.

2.4 Pre-Bid Compliance Process

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

2.4.1.1 [draft technical bids/draft responses to the mandatory technical requirements]

This is referred to as a "**Pre-Bid**". The submission of a Pre-Bid by any bidder is optional and is not a pre-condition to submitting a bid on the closing date. Canada will not return Pre-Bids to bidders, but will treat Pre-Bids the same way it treats bids, in accordance with Section 1.8(j) of SSC's Standard Instructions.

2.4.2 **How to submit a Pre-Bid**:

2.4.2.1 by email to the Contracting Authority. When a Pre-Bid is received by email, the Contracting Authority will send an email acknowledgement back to the bidder. If the bidder does not receive an email acknowledgement, the bidder is encouraged to follow-up by telephone with the Contracting Authority.

2.4.3 **A Pre-Bid will only be reviewed if submitted by the Pre-Bid Deadline**: Canada will review only Pre-Bids submitted by no later than 11:59 p.m. [Month Day, 2022] (the "**Pre-Bid Deadline**"). Canada will review only one Pre-Bid from each bidder (i.e. after receiving feedback, the bidder cannot submit a new version of its Pre-Bid for review).

2.4.4 **Canada will provide Feedback on Pre-Bids**: The Contracting Authority will provide confidential feedback, referred to as a Preliminary Evaluation Notice (PEN), to each bidder that has submitted a Pre-Bid by the Pre-Bid Deadline. Canada will normally provide that feedback by email and the bidder is deemed to have received Canada's feedback at the time it is sent by Canada. Canada is not responsible for any technical delays in the receipt by the bidder of its feedback.

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

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

2.4.6.1 have not been addressed at all;

2.4.6.2 have not been sufficiently addressed; and

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

While Canada will note the reason the Pre-Bid is deficient, Canada will not indicate to the bidder how the deficiency can be corrected. For example, the feedback might consist of statements such as the following:

2.4.6.3.1 The OEM certification appears to have been signed by a representative of the bidder rather than the OEM.

2.4.6.3.2 The Pre-Bid did not demonstrate that the bidder has 3 years of experience on the Pre-Bid closing date.

2.4.6.3.3 The Pre-Bid did not demonstrate that proposed equipment meets the specifications set out in Annex B.

2.4.6.3.4 The Pre-Bid did not demonstrate that the bidder has an existing portal for placing service orders.

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

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

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

NO FINANCIAL INFORMATION: CANADA REQUESTS THAT BIDDERS NOT INCLUDE ANY FINANCIAL INFORMATION IN THEIR PRE-BID.

2.5 Volumetric Data

2.5.1 The unprecedented evolution of conferencing technology has occurred swiftly to respond to the needs of citizens worldwide during the pandemic. As such, the following data has been provided to Bidders, showing the vast differences in volumetrics for operator assisted conferences pre-pandemic, and during pandemic. Canada does not estimate trends in operator assisted usage as technology has evolved including partially or fully automated technological features to accommodate many of the legacy operator assisted functions/responsibilities. Canada recognizes that operator resources deliver a service unparalleled to the operator functionality offered by the SaaS

conferencing application platform, and as such, when required, operator resources are paramount to SaaS operator functions/responsibilities. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of the operator-assisted conferencing services will be consistent with this data. It is provided purely for information purposes.

2.5.2 It is difficult to estimate the utilization for Operator Assisted Services in the post-pandemic environment; however, pre-pandemic are reflected below.

2.5.3 The size of conferences before the COVID-19 pandemic typically were:

- 93 connections per conference
- 30% of the conferences are between 100 and 400 connections
- 22%, between 40 and 100 connections
- 30%, between 10 and 40 connections
- 18%, under 10 connections

2.5.4 As a result of the pandemic, the current Operator Assisted Service has been exclusively used for pandemic response purposes by key Government officials. The size of conferences during the pandemic are typically:

- 44 connections per conference
- 89% of the conferences are between 1 and 100 connections
- 9%, between 100 and 400 connections
- 1%, between 400 and 700 connections
- >1%, for conferences over 700 connections

2.5.5 The following are volumetrics for percentage of ports used versus ports reserved for Operator Assisted conferences post pandemic.

Month/Year	Ports Reserved	Actual Ports	Percentage Used
2021			
November 2021	8998	4218	46.88%
December 2021	16340	4316	26.41%
2022			
January 2022	4555	1405	30.85%
February 2022	15625	5241	33.54%
March 2022	10948	3189	29.13%
April 2022	13418	2796	20.84%
May 2022	8827	1726	19.55%
June 2022	12899	2616	20.28%
July 2022	2325	529	22.75%
August 2022	3072	542	17.64%
September 2022	3850	770	20.00%
October 2022	9517	1377	14.47%

2.5.6 The following are volumetrics for number of minutes consumed and the average minutes per meeting as a sampling of pre- pandemic, during pandemic, and post pandemic.

Month/Year	# of Meetings	# of Minutes	Average Minutes per Meeting
2019 – Pre-pandemic			
April	304	212,732.00	699.78
May	376	476,029.00	1,266.03
June	383	470,702.00	1,228.99
July	237	235,985.00	995.72
August	179	140,079.00	782.56
September	210	255,618.00	1,217.23
October	212	232,513.00	1,096.76
November	243	332,915.00	1,370.02
December	219	299,914.00	1,369.47
2020 - Pandemic			
January	243	217,132.00	893.55
February	317	293,604.00	926.2
March	673	1,421,645.00	2,112.40
April	686	1,570,907.00	2,289.95
May	493	888,747.00	1,802.73
June	491	524,084.00	1,067.38
July	237	350,439.00	1,478.65
August	179	433,539.00	2,422.01
September	214	312,699.00	1,461.21
October	236	367,825.00	1,558.58
November	207	382,708.00	1,848.83
December	188	585,543.00	3,114.59
2021 – Pandemic			
January	142	318,978.00	2,246.32
February	211	257,200.00	1,218.96
March	208	306,486.00	1,473.49
April	191	262,133.00	1,372.42
May	174	147,310.00	846.61
June	257	211,380.00	822.49
July	81	89,993.00	1,111.02
August	45	46,824.00	1,040.53
September	39	41,739.00	1,070.23
October	47	159,496.00	3,393.53
November	102	173,391.00	1,699.91
December	149	110,652.00	742.63

2022 – Post-pandemic			
January	70	71,809.00	1,025.84
February	164	184,935.00	1,127.65
March	106	121,967.00	1,150.63

2.5.7 SSC acknowledges that the above metrics are lower than the pre-pandemic usage shown. This is primarily due to the exclusive use of the existing operator-assisted conferences for the pandemic response.

2.5.8 The scalability of the conferencing environment is an essential requirement of the service, as witnessed during the pandemic or any other national emergency situation or crisis. To address the pandemic, Canada rapidly deployed changes to the framework of existing conferencing services to meet the GC's needs in an emergency response.

2.6 Questions and Comments

2.6.1 Questions and comments about the solicitation must be submitted to the Contracting ` by the date and time specified below. Canada may not respond to questions submitted to someone other than the Contracting Authority. Questions and comments received after the deadline may not be answered.

2.6.2 The deadline for submitting questions and comments to the Contracting Authority is MONTH DD, YYYY @ 02:00 PM (ET).

2.6.3 Bidders should reference as accurately as possible the numbered item of the RFP to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must 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 the Bidder do so, so that the proprietary nature of the question(s) is eliminated, and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.7 Applicable Laws

2.7.1 The resulting contract(s) must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

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

2.8 Code of Conduct for Procurement

2.8.1 The PSPC Code of Conduct for Procurement, which SSC adopts for the purposes of this solicitation, provides that bidders must respond to bid solicitations in an honest, fair and comprehensive manner, accurately reflect their capacity to satisfy the requirements set out in the bid solicitation and resulting contract, submit bids, and enter into contracts only if they will fulfill all obligations of the contract. By submitting a bid, the bidder is certifying that it is complying with the ***Code of Conduct for Procurement***. Failure to comply with the ***Code of Conduct for Procurement*** may render the bid non-compliant.

2.9 Bid Challenge and Recourse Mechanisms

2.9.1 Several mechanisms are available to potential suppliers to challenge aspects of the procurement process up to and including contract award.

2.9.2 Canada encourages suppliers to first bring their concerns to the attention of the Contracting Authority. Canada's Buy and Sell website, under the heading "Bid Challenge and Recourse Mechanisms" contains information on potential complaint bodies such as:

2.9.2.1 Office of the Procurement Ombudsman (OPO);

2.9.2.2 Canadian International Trade Tribunal (CITT).

2.9.3 Suppliers should note that there are strict deadlines for filing complaints, and the time periods vary depending on the complaint body in question. Suppliers should therefore act quickly when they want to challenge any aspect of the procurement process.

PART 3 BID PREPARATION INSTRUCTIONS

3.1 General Instructions

3.1.1 SSC's Standard Instructions include instructions with respect to bids, which apply in addition to those described in this document. If there is a conflict between the provisions of SSC's Standard Instructions and this document, this document prevails.

3.2 Bid Preparation Instructions

3.2.1 Canada requests that the Bidder submits its bid in separately bound sections as follows:

3.2.1.1 Section I: Technical Bid

3.2.1.2 Section II: Financial Bid

3.2.1.3 Section III: Certifications and Additional Information

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

3.3 Section I: Technical Bid

3.3.1 Bidders must submit the Mandatory Technical Evaluation Form at [Annex/Appendix X] as part of their technical bid. In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability and describe their approach in a thorough, concise and clear manner for carrying out the work.

3.3.2 The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. To facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

3.3.3 The technical bid may refer to additional documentation submitted with the bid. Valid forms of technical documentation reference material include, but are not limited to:

3.3.3.1 screen captures, clearly legible, with text explanations; and

3.3.3.2 technical or end-user documentation. Where the documentation is stored within a website, the Bidder must extract the supporting information and insert it in the bid or attach the documentation as an annex. The Bidder must clearly indicate what portions of the text (pages and paragraphs) provide the demonstration required.

3.3.4 Canada will not accept and will not consider for the bid evaluation purposes any information that is referenced to a URL and requires Canada to download information from an Internet site, unless specifically allowed (for example, Corporate web-site, Product List URL).

3.3.5 If during bid evaluation it becomes apparent that the contact information for any customer references is incorrect, the Bidder will be permitted to provide the correct address, telephone number, fax number or e-mail address. If the customer reference is unavailable when required during the evaluation period, Canada will contact the back-up customer reference from the same customer organization. Bidders will not be

permitted to submit an alternate customer organization or customer reference within the same customer organization after Solicitation Closing.

3.4 Section II: Financial Bid

3.4.1 Bidders must submit their financial bid in the Pricing Tables contained in the COAS Financial Evaluation Workbook, and it must be in the original Excel format rather than a PDF. Bidders must quote firm unit prices in Canadian dollars.

3.5 Section III: Certifications and Additional Information

3.5.1 Bidders must submit the certification and additional information required under Part 5 – Certifications and Additional Information.

PART 4 EVALUATION PROCESS

4.1 General Evaluation Procedures

4.1.1 General evaluation procedures that apply to this solicitation are described in SSC's Standard Instructions for Procurement, Version 1.4.

4.1.2 A bid must comply with all the requirements of the solicitation, meet all mandatory evaluation criteria, pass all pass/fail evaluation criteria to be declared compliant.

4.1.3 An evaluation team composed of representatives of Canada will evaluate the bids.

4.1.4 Any bid that does not follow the requested format and instructions as defined in this Request for Proposal or does not provide a complete bid, shall be declared non-compliant and shall not be given any further consideration.

4.1.5 **Requests for Clarifications:** If Canada seeks clarification from the Bidder about its bid, the Bidder will have 2 FGWDs (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive. If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

4.1.6 By submitting a bid, the Bidder certifies that the Bidder is responsive to all mandatory requirements.

4.1.7 **Evaluation Team:** An evaluation team composed of representatives of Canada will evaluate the RFP bids. Canada may hire any independent consultant, or use any Government resources, to evaluate any RFP bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

4.1.8 **Compliance Determination:** Once the evaluators have completed their evaluation and documented findings on the technical evaluation sheets, the results are to be reviewed by the Contracting Authority. If the team members have differed in their evaluation of the mandatory requirements, a consensus meeting is held, and a final determination is made by consensus for each criterion for which a discrepancy existed.

4.1.9 **Discretionary Rights during Evaluation:** In conducting its evaluation of the bids, Canada may, but will have no obligation to, do the following:

4.1.9.1 request additional information substantiating the compliance of the Bid with any mandatory requirement, if that substantiation was not required to be included in the bid on the closing date.

4.1.9.2 seek clarification from Bidders regarding any or all information provided by them with respect to the solicitation.

4.1.9.3 request specific information with respect to any Bidders legal status.

4.1.10 With respect to the provisions of Section 1.13 of the Standard Instructions, Canada will require a demonstration from the 1st, 2nd and 3rd top-ranked bidder, in accordance with the Demonstration Obligations in the COAS Technical Requirements Evaluation Workbook.

4.2 Security Requirements

4.2.1 The Bidder will be evaluated with respect to the mandatory security requirements as further described in section 1.3:

4.2.1.1 the CSP ITS Assessment;

4.2.1.2 the SCI Assessment;

4.2.1.3 the Contract Security Program (SRCL).

4.2.2 These requirements, including meeting the acceptable risk level, and the security clearance apply at the time of contract award. If SSC is ready to award the contract, but has not yet received all the information required to demonstrate that the Bidder meets the requirements, SSC will provide the Bidder with 5 working days to submit the outstanding documents. After that time, whether or not to delay the award is entirely within the discretion of SSC.

4.3 Technical Evaluation - Mandatory Technical Criteria

4.3.1 Each bid will be reviewed to determine whether it meets the mandatory requirements of the bid solicitation. Any element of the bid solicitation identified with the words "must" or "mandatory" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

4.3.2 Claims in a bid that a future upgrade or release of any of product included in the bid will meet the mandatory requirements of the bid solicitation, where the upgrade or release is not available at bid closing, will not be considered.

4.3.3 Technical bids will be evaluated in accordance with Attachment 4.1: COAS Mandatory (Pass/ Fail and Mandatory Rated) Technical Requirements Evaluation Workbook.

4.3.4 If the technical evaluation tables provided to bidders include any formulae, Canada may re-input the values provided by Bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a Bidder.

4.3.5 **Attachment 4.1: COAS Mandatory Technical Requirements Evaluation Workbook includes:**

4.3.5.1 Worksheets M-1 to M-4 inclusive will be evaluated as Pass or Fail based on completion and content of responses, and responses from customer reference checks.

4.3.5.2 The Bidder's response to R-1, Design Documentation baselines the Contractor's high level design and implementation plan at contract award and will be evaluated based on a rated score

4.3.5.3 The Technical Evaluation Worksheet includes the results for all Mandatory Technical Criteria and Customer Reference responses.

4.4 Financial Evaluation

4.4.1 Financial bids will be evaluated in accordance with Attachment 4.2 : COAS Financial Evaluation Workbook.

4.4.2 The financial evaluation will be conducted by calculating the ranking of all Bidders, in accordance with the tab entitled Evaluation of the COAS Financial Evaluation Workbook using the pricing for the tabs entitled 1. OAS; 2. Audio Web, and 3. Service Portal, completed by the bidders.

4.4.3 **Formulae in Pricing Tables**

If the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a bidder.

4.5 Basis of Selection

4.5.1 A bid must comply with the requirements of the bid solicitation and meet all mandatory evaluation criteria to be declared responsive.

4.5.2 Although Canada will award only one contract, the responsive bids, ranked 1st, 2nd and 3rd are required to pass the Demonstration Obligation,

4.5.3 Bidders that pass the Demonstration Obligation will be required to proceed with:

4.5.3.1 the CSP ITS assessment;

4.5.3.2 the SCI assessment;

4.5.3.3 the Contract Security Program (SRCL).

4.5.4 The highest ranked bidder, that passes the Demonstration Obligations, the Contract Security Program, and meets all security requirements, with the risk level of medium or lower for the SCI Assessment and the CSP IT**S** Assessment will be recommended for contract award.

4.5.5 Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract.

4.5.6 Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

PART 5 ADDITIONAL INFORMATION

5.1 Additional Information Required with the Bid

5.1.1 Bid Submission Form

Bidders must provide a duly completed Bid Submission Form with their bids. It provides a common form in which Bidders can provide information required for evaluation and contract award such as: contact name, Procurement Business Number, the Bidder's status under the Federal Contractor's Program for Employment Equity, legal names of Joint Venture members, etc. Using the form to provide the information requested is not mandatory, but it is recommended.

5.2 Certifications Precedent to Contract Award and Additional Information

5.2.1 The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.2.2 Certifications Requested at Solicitation closing, (Mandatory upon request):

By submitting a bid, the Bidder is automatically providing the certifications identified below as "required". The content of each certification is set out in SSC's Standard Instructions in the section entitled "**Deemed Certifications from Each Bidder**":

If the table below indicates that a certification is requested, the Bidder is required to provide the following certifications described in SSC's Standard Instructions. Although all these certifications are requested at Bid closing, if Canada determines that any certification is missing, incomplete or requires correction, Canada will provide the Bidder with an opportunity to provide the required information. Providing the certification when requested during the evaluation period is mandatory.

Equipment and Software is "Off-the-Shelf"	Required
System is "Off-the-Shelf"	Required
Bidder's Proposed Resources will be available	Required
Bidder has Verified Information about its Proposed Resources	Required

5.2.3 Integrity Provisions – Required Documentation

5.2.3.1 In accordance with the Ineligibility and Suspension Policy, the Bidder must provide the required documentation, as applicable. Consult sections 4.21, 5.16 and 8.70.2 of the Supply Manual for additional information.

5.2.3.2 In accordance with the section titled Information to be provided when bidding, contracting or entering into a real property agreement of the Ineligibility and Suspension Policy (http://www.tpsgc-pwgsc.gc.ca/ci-if/politique-policy-

eng.html), the Bidder must provide the required documentation, as applicable, to be given further consideration in the procurement process.

5.2.4 Integrity Check (Requested at Solicitation closing, Mandatory upon request):

5.2.4.1 Bidders are requested to include a completed Form XX – Integrity Check with their bids. Using the form to provide the information is not mandatory, but it is recommended. If Form XX is not included with the bid or if Canada determines that the information required by Form XX is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so. Upon request, the Bidder must also provide any further information required by the Contracting Authority pursuant to Section 1 SSC's Standard Instructions.

5.2.5 **Federal Contractors Program for Employment Equity – Bid Certification**

5.2.5.1 By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list available at the bottom of the page of the Employment and Social Development Canada (ESDC) - Labour's website.

5.2.5.2 Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid list at the time of contract award.

5.2.5.3 Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

5.2.5.4 The Bidder must provide the Contracting Authority with a completed annex titled Federal Contractors Program for Employment Equity - Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

5.2.6 **Certifications Required by Supplemental Standard Instructions 2003-1:**

5.2.6.1 Bidders are required to submit the required regulatory certifications in accordance with Supplemental Standard Instructions - Telecommunications. Bidders should note that only tariffs to which the Bidder itself will be subject in performing the work are required to be submitted. It is the responsibility of the Bidder to manage its own relationship with any subcontractors who may be subject to tariffs.

5.2.6.2 **CSP ITS Assessment Submission (If Requested post-evaluation, Mandatory upon request within 5 FGWDs)**:

The Bidder's Cloud Service Provider, if requested to the Bidder, must submit a completed ISO 27001 **OR** SOC 2 Type II report, and a completed ITSM.50.062 Cloud Security Risk Management of Tier 1 (PA LL) for the services required to deliver the COAS. if Canada determines that the information required is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so. Upon request, the Bidder must also provide any further information required by the Contracting Authority pursuant to Section 1 SSC's Standard Instructions.

5.2.6.3 **Supply Chain Security Integrity (SCSI) (If Requested post-evaluation, Mandatory upon request within 5 FDGWDs)**:

The Bidder, if requested, must submit a completed SCI Submission as per Annex G for the services required to deliver the COAS.

5.2.6.3.1 the list of IT Products, cloud service providers, and subcontractors (which will become Annex G at contract award), as required in the Article entitled IT Product List of Appendix 1 to Annex G - Supply Chain Security Information Assessment Process.

5.2.6.3.2 if Canada determines that the information required is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so. Upon request, the Bidder must also provide any further information required by the Contracting Authority pursuant to Section 1 SSC's Standard Instructions.

5.2.6.3.3 By submitting a bid, the Bidder confirms its agreement to the terms and conditions of the Non-Disclosure Agreement set out in Appendix 1 to Annex G – Supply Chain Security Information Assessment Process.

5.2.6.4 **Greenhouse Gas (GHG) Emissions Reduction**

Bidders are requested to provide a report detailing their level of participation (i.e., greenhouse gas (GHG) emissions reduction target set in-line with the Paris Agreement or net-zero 2050 target set) from either:

5.2.6.4.1 an independent third party recognized by and acceptable to SSC, including but not limited to the Science Based Targets Institute; or

5.2.6.4.2 Environment and Climate Change Canada's Net-Zero Challenge.

PART 6 SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6. Security Requirements

6.1.1 Before award of a contract, the following conditions must each be met:

6.1.1.1 the Bidder's Cloud Service Provider (CSP) IT assessment must obtain a risk rating of medium, or lower.

6.1.1.2 the Bidder's SCI assessment must obtain a risk rating of medium, or lower.

6.1.1.3 the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

6.1.1.4 the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work sites must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses; and

6.1.1.5 the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites.

6.1.1.6 Bidders are reminded to obtain the required security clearance promptly. Any delay in the award of a contract to allow the successful Bidder to obtain the required clearance will be at the entire discretion of the Contracting Authority.

6.1.1.7 For additional information on security requirements, Bidders should refer to *Error! Reference source not found.*and to the **Contract Security Program of Public Works and Government Services Canada** https://www.tpsgc-pwgsc.gc.ca/esc-src/introduction-eng.html website.

PART 7 RESULTING CONTRACT CLAUSES

Note to Bidders: These Resulting Contract Clauses are intended to form the basis of any contract resulting from this bid solicitation. Except where specifically set out in these Resulting Contract Clauses, acceptance by Bidders of all the clauses is a mandatory of this bid solicitation.

No modification or other terms and conditions included in the bid will apply to the resulting contract, despite the fact that the bid may become part of the resulting contract.

Any Bidder submitting a bid containing statements implying that the bid is conditional on modification of these Resulting Contract Clauses (including all documents incorporated by reference) or containing terms and conditions that purport to supersede these Resulting Contract Clauses will be considered non-compliant.

Bidders with concerns regarding the provisions of these Resulting Contract Clauses should raise those concerns in accordance with the Enquiries provision of the bid solicitation.

If additional legal issues are raised by a bid, Canada reserves the right to address those issues in any contract awarded as a result of this bid solicitation. If the additional provisions are unacceptable to the Bidder, the Bidder may withdraw its bid.

7.1 Requirement

7.1.1 "This is a contract between _____(the "Contractor") and His Majesty the King in Right of Canada, as represented by the Minister of State (Public Services and Procurement), who presides over Shared Services Canada ("Canada"), for the provision of Conferencing and Operator Assisted Services (COAS).

7.1.2 _____ (the Contractor) agrees to supply to the Client the Conferencing and Operator Assisted Services described in the Contract, including the Statements of Work, Annexes A, B and C in accordance with, and at the prices set out in, the Contract. As part of the Work, the Contractor must:

7.1.2.1 provide a fully managed Audio/Web Conferencing Service as described in the Contract, as and when requested;

7.1.2.2 provide a fully managed Operator Assisted Service as described in the Contract, as and when requested;

7.1.2.3 develop and provide access to a fully managed bilingual and secure portal, inclusive of training on the use of the portal, as described in the Contract;

7.1.2.4 provide Service Desk support, as described in the Contract;

7.1.2.5 provide the Reports and Service documentation, as described in the Contract;

7.1.2.6 secure all consents and intellectual property rights (including licensing rights) that may be necessary in order to deliver COAS; and

7.1.2.7 design, provide, manage, configure, support and maintain all the hardware, software and firmware it uses to deliver Services as required to meet all the requirements of the Contract. Given that the Contractor is providing a managed service, Canada acknowledges that the Contractor retains ownership (or is the licensee, as the case may be) for all hardware, software and firmware that the Contractor uses to perform the Work.

7.1.2.8 providing tutorial/training, as and when requested by Canada.

7.1.3 The Contractor acknowledges that *[To be inserted at contract award]* **(the "second-ranked Bidder")** submitted a bid in response to the COAS RFP that Canada determined was fully compliant and ranked second according to the evaluation methodology in the COAS RFP. If this Contract is terminated for default any time during the 360 Federal Government Work days following the award of this Contract, Canada may, in its absolute discretion, award a new contract for COAS to the second-ranked Bidder, if the second-ranked Bidder confirms to Canada that it will honour its bid (regardless of whether that bid has otherwise expired). Pursuant to any such new contract, the second-ranked Bidder will be subject to the same requirements established under this Contract and must obtain acceptance for Operational Readiness before it can start delivering any Services.

7.2 Clients, Partners, and Subscriber

7.2.1 **Clients**: SSC is a shared services provider within the Government of Canada. At any point during the Contract Period SSC's "**Clients**" include:

7.2.1.1 SSC itself;

7.2.1.2 Partners**:** government institutions for which SSC services are Mandatory and who are signified to use SSC services as Mandatory in the legend at http://service.ssc-spc.gc.ca/en/policies_processes/pin-2016-01/appendix-a; and

7.2.1.3 those other organizations for whom SSC's services are optional and that choose to use those services from time to time.

For the purposes of invoicing, the Client "SSC" refers to SSC themselves as a department, and Partners (SSC and Partners are invoiced together directly to SSC).

7.2.2 **Subscriber:** The term "**Subscriber**" includes any individual scheduling or hosting an audio/web conference or an Operator-assisted conference or on behalf of a Client for Services under this Contract, whether that individual is an employee, consultant, contractor or agent, and has the meaning given to it in Annex A. A specific "Subscriber" is the individual whom registers for a conferencing account through the Contractor's Service Portal.

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

7.3 Evolution of Services

7.3.1 In light of the fact that technology and business models evolve quickly in the network services market, the Contractor acknowledges that Canada's intention is to offer robust, comprehensive, and up-to-date Services to its users throughout the Contract Period.

7.3.2 The Contractor agrees to offer all improvements it is offering to any other customer as part of its standard Audio/Web and Operator Assisted conferencing services, at no additional charge to Canada. For improvements to Services that the Contractor is not offering to its other customers as part of its standard audio, web and Operator Assisted conferencing services, the parties may agree to add these improvements (including but not limited to new web conferencing services, accessibility services) negotiated on a case-by-case basis

and, if successfully concluded, will be documented by a formal Contract Amendment issued by the Contracting Authority. These improvements may include, among other things, discounts resulting from aggregating certain services or discounted pricing for additional capacity. Where the Basis of Payment is affected by any negotiated changes to the Service, Canada may require the Contractor to substantiate the proposed pricing, as described in article **Prices to be Negotiated**.

7.3.3 The Contractor is responsible for all enhancements, expansions, and upgrades that are necessary to maintain robust, comprehensive, and up-to-date Services during the term of the Contract.

7.3.4 The Contractor agrees to advise the Technical Authority of all technological (including without limitation technological enhancement, augmentation or replacement,) administrative and commercial improvements that affect Services and, on Canada's request, implement improvements recommendations for all processes and procedures.

7.3.5 Service Catalogue Items can be added to the Service Catalogue (Annex E) and described in Appendix 1 to Annex E for new Service features and functionalities. The price of these Service Catalogue updates will be negotiated on a case-by-case basis (as set out in the Article entitled "Basis of Payment") and, if accepted by Canada, will be reflected in a Contract Amendment.

7.3.6 Whether or not to accept or reject a proposed improvement is entirely within the discretion of Canada. If Canada does not agree to a proposed improvement, the Contractor must continue to deliver the original Service(s) as and when requested by Canada. If accepted, any improvement to the Services will be documented for the administrative purposes of Canada by a Contract Amendment adding the improvement to the Contract as a Service Catalogue Item available for purchase or by revising the terms and conditions to reflect an enhancement to an existing Service Catalogue Item.

7.4 Contract Period & Options

7.4.1 **Contract Period**: The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

7.4.1.1 The period from the Contract Award Date, which is the date on which the Contract is issued as shown on page 1 of this Contract (unless Work is delayed as a result of a pending tariff approval, in which case the Work will begin once Work proceeds in accordance with the Article entitled "Status of Contract Pending Final Approval from CRTC" in Supplemental General Conditions 4005), until the In-Service Date;

7.4.1.2 The "**Initial Contract Period**", which begins on the In-Service Date, and ends 4 year(s) later; and

7.4.1.3 The period during which the Contract is extended, if Canada chooses to exercise any options set out in the Contract.

7.4.2 **Option to Extend the Contract**:

7.4.2.1 The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to 6 additional one-year period(s) under the same terms and conditions.

7.4.2.2 The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

7.4.2.3 Canada may exercise this option at any time by sending a written notice to the Contractor at least 30 calendar days before the expiry date of the Contract. The

option may only be exercised by the Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

7.5 Branding

7.5.1 Canada will develop the brand for COAS, which may consist of a name, sign, symbol, slogan or anything that can be used to identify and distinguish COAS.

7.5.2 The Contractor must implement the COAS brand as specified by Canada, including by putting the brand identification on:

7.5.2.1 portal landing pages;

7.5.2.2 web pages;

7.5.2.3 Web-based Graphical User Interfaces (GUIs).

7.5.2.4 documentation; and

7.5.2.5 reports.

7.5.3 The Contractor must not use its brand with the exception of any brands or logos from commercial-off-the-shelf products in use by the Contractor where the Contractor is unable to remove the brand or logo.

7.5.4 Canada will retain all rights to the COAS brand during the Contract period and after expiry or termination of the Contract. Upon request, the Contractor will transfer to Canada or its designates Internet domain names established for providing Services under this Contract when and as requested by the TA, at least 30 calendar days prior to expiration or termination of the Contract (or a later date agreed to by the TA in writing) at no cost to Canada.

7.6 Defined Terms

7.6.1 Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions of Supplemental General Conditions. In addition, the words set out below have meanings set out there. Other terms are also defined elsewhere in this Contract, including the Statement of Work.

7.6.1.1 **Contract Award Date:** The date on which the Contract is awarded, as shown on page 1 of this Contract.

7.6.1.2 **In-Service Date:** The In-Service date is the date the Contractor must have met and received SSC Operational Readiness acceptance for all obligations required by the In-Service dates in the Statement of Work, Annex A.

7.6.1.3 **Federal Government Working Days (FGWDs)**: "Federal Government Working Days (FGWDs)" means Monday to Friday excluding the following holidays as observed by the Government of Canada:

7.6.1.3.1 New Year's Day;

7.6.1.3.2 Good Friday and Easter Monday;

7.6.1.3.3 Victoria Day;

7.6.1.3.4 St Jean Bapiste (Quebec only);

7.6.1.3.5 Canada Day;

7.6.1.3.6 1st Monday in August (not in Quebec);

7.6.1.3.7 Labour Day;

7.6.1.3.8 National Day for Truth and Reconciliation;

7.6.1.3.9 Thanksgiving Day;

7.6.1.3.10 Remembrance Day;

7.6.1.3.11 Christmas Day; and

7.6.1.3.12 Boxing Day.

7.7 Standard Clauses and Conditions

7.7.1 **Incorporation by Reference**: All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (http://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Services and Procurement Canada. These clauses and conditions are incorporated by reference into and form part of this Contract as though they were set out here in full. All references contained within the General Conditions to the Minister of Public Services and Procurement of Canada will be interpreted as a reference to the minister presiding over Shared Services Canada and all references to the Department of Public Works and Government Services or to Public Services and Procurement Canada will be interpreted as references to Shared Services Canada.

For purposes of this Contract, the PWGSC policies referenced within the Standard Acquisitions Clauses and Conditions Manual are adopted as SSC policies.

7.7.2 **General Conditions:** 2035 (bearing the most recent date on or before the date this contract was issued), General Conditions - Higher Complexity - Services, apply to and form part of the Contract. These General Conditions are amended as follows:

7.7.2.1 Section 2, Section 2 is deleted and replaced with the following:
The clauses and conditions identified by number, date and title in the Contract are incorporated by reference and form part of the Contract as though expressly set out in the Contract;

7.7.2.2 in Subsection 6(1), delete the words "Except as provided in subsection 2" and capitalize the first word remaining in that sentence;

7.7.2.3 the text of Subsection 6(2) is deleted;

7.7.2.4 in Subsection 6(3), delete the words "other than a subcontract referred to in paragraph 2(a)"; and

7.7.2.5 in the case of a termination for convenience under Section 30, the next placed financial-ranked Alternate contractor will move up accordingly. For example, if the Primary Contractor's contract is terminated for default, the next placed financial-ranked Alternate Contractor will automatically become the Primary Contractor.

7.7.3 **Supplemental General Conditions:** The following Supplemental General Conditions apply to and form part of the Contract.

7.7.3.1 4005 (bearing the most recent date on or before the date this contract was issued), Supplemental General Conditions – Telecommunications Services and Products;

7.7.3.2 4006 (bearing the most recent date on or before the date this contract was issued) Supplemental General Conditions – Intellectual Property Rights in Foreground Information;

7.8 Security Clearance and the CISD Requirements for Canadian Contractor

7.8.1 The following security clauses and the security requirements checklist (SRCL), Annex D applies and forms part of the Contract.

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

7.8.1.2 The Contractor/Offeror personnel requiring access to PROTECTED information, assets or site(s) must EACH hold a valid RELIABILITY STATUS, granted or approved by the CSP, PWGSC.

7.8.1.3 The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until the CSP, PWGSC has issued written approval. After approval has been granted or approved, these tasks may be performed at the level of PROTECTED A.

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

7.8.1.5 The Contractor/Offeror must comply with the provisions of the:

7.8.1.5.1 Security Requirements Check List and security guide (if applicable), attached at Annex D;

7.8.1.5.2 Contract Security Manual (Latest Edition).

7.9 Security Clearance and the CISD Requirements for Foreign Contractor

7.9.1 The following security requirements apply to the foreign recipient Contractor incorporated or authorized to do business in a jurisdiction other than Canada and delivering outside of Canada the services listed and described in the subsequent Contractor.

7.9.2 The Foreign recipient Contractor must, at all times during the performance of the Contract, hold an equivalence to a valid Designated Organization Screening (DOS), issued by the Canadian DSA as follows:

7.9.2.1 The Foreign recipient Subcontractor must provide proof that they are incorporated or authorized to do business in their jurisdiction.

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

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

7.9.2.4 The Foreign recipient Contract/Subcontract must not grant access to CANADA PROTECTED A information/assets, except to its personnel subject to the following conditions:

7.9.2.4.1 Personnel have a need-to-know for the performance of the Contract;

7.9.2.4.2 Personnel have been subject to a Criminal Record Check, with favourable results, from a recognized governmental agency or private sector organization in their country as well as a Background Verification, validated by the Canadian DSA;

7.9.2.4.3 The Foreign recipient Contractor must ensure that personnel provide consent to share results of the Criminal Record and Background Checks with the Canadian DSA and other Canadian Government Officials, if requested; and

7.9.2.4.4 The Government of Canada reserves the right to deny access to CANADA PROTECTED information/assets to a foreign recipient Contractor for cause.

7.9.2.5 CANADA PROTECTED information/assets provided or generated pursuant to this Contract must not be further provided to a third party Foreign recipient Subcontractor unless:

7.9.2.5.1 written assurance is obtained from the Canadian DSA to the effect that the third-party Foreign recipient Contractor has been approved for access to CANADA PROTECTED information/assets by the Canadian DSA; and

7.9.2.5.2 written consent is obtained from the Canadian DSA, if the third-party Foreign recipient Contractor is located in a third country.

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

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

7.9.3 **DSC**

7.9.3.1 The Foreign recipient Subcontractor must, at all times during the performance of the Contract hold an equivalence to an approved Document Safeguarding Capability (DSC) at the level of CANADA PROTECTED A.

7.9.4 All CANADA PROTECTED information/assets, furnished to the foreign recipient Contractor or produced by the foreign recipient Subcontractor, must also be safeguarded as follows:

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

7.9.4.2 The Foreign recipient Contractor must immediately report to the Canadian DSA all cases in which it is known or there is reason to suspect that CANADA PROTECTED information/assets accessed by the foreign recipient Contractor, pursuant to this Contract, have been lost or disclosed to unauthorized persons.

7.9.4.3 The Foreign recipient Contractor must not disclose CANADA PROTECTED information/assets to a third party government, person, firm or representative

thereof, without the prior written consent of the Government of Canada. Such consent must be sought through the Canadian DSA.

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

7.9.4.5 The Foreign recipient Contractor must, at all times during the performance of this Contract, ensure the transfer of CANADA PROTECTED information/assets be facilitated through the Canadian DSA.

7.9.4.6 Upon completion of the Work, the foreign recipient Contractor must return to the Government of Canada, all CANADA PROTECTED information/assets furnished or produced pursuant to this Subcontract, including all CANADA PROTECTED information/assets released to and/or produced by its Contractors.

7.9.5 **IT**

7.9.5.1 The Foreign recipient Contractor MUST NOT utilize its Information Technology (IT) systems to electronically process, produce, or store on a computer system any CANADA PROTECTED A information/assets until authorization to do so has been confirmed by the Canadian DSA.

7.9.5.2 See Annex D for security measures required for the treatment and access to CANADA PROTECTED A information/assets.

7.9.5.3 The Foreign recipient Contractor must ensure that all the databases, including backup databases used by organizations to provide the services described in the SOW containing any CANADA PROTECTED information, related to the Work, are located within Canada.

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

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

7.9.5.6 The Foreign recipient Contractor must comply with the provisions of the Security Requirements Check List attached at Annex D.

7.9.5.7 Canada has the right to reject any request to electronically access, process, produce, transmit or store CANADA PROTECTED information/assets related to the Work in any other country if there is any reason to be concerned about the security, privacy, or integrity of the information.

7.10 Authorities

7.10.1 **Contracting Authority:** The Contracting Authority for the Contract is:

Name	Eric Vanasse
Title	Senior Procurement Officer
Address	400 Cooper St, Flr 6, Ottawa, ON
Telephone Number	514-607-8519
Email Address	Eric.Vanasse@ssc-spc.g.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The

Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

7.10.2 **Technical Authority:** The Technical Authority for the Contract is:

<To be inserted at Contract Award>

Name	
Title	
Address	
Telephone Number	
Fax Number	
Email Address	

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

7.10.3 **Contractor's Representative:**

<To be inserted at Contract Award>

Name	TBD
Title	
Address	
Telephone Number	
Fax Number	
Email Address	

7.11 Basis of Payment

7.11.1 For providing the Conferencing and Operator Assisted Services, in accordance with the Contract, Canada will pay the Contractor according to the firm unit prices in Annex E.

7.11.1.1 **Per-minute usage**: For providing the operator assisted services in core and non-core hours, emergency conferences and events, in accordance with the Contract, Canada will pay the Contractor the usage based on the firm per-minute prices set out in Annex E, multiplied by the number of active ports used, and multiplied by the total minutes consumed, the Applicable Taxes extra.

7.11.1.2 **Per Flat Rate Fee COAS Service:** For providing flat rate fee COAS services (includes features and functions of the Audio/Web, and unused ports if reserved, but with zero minutes usage)**:** For providing the flat rate fee COAS services, in accordance with the Contract, Canada will pay the Contractor the usage based on the unit price flat rate fee set out in Annex E, multiplied by the number of times the COAS flat rate fee service was consumed, the Applicable Taxes extra.

7.11.1.3 **Per Active User Audio/Web Annual License Fee**: For providing the per Active User audio/web annual licenses in accordance with the Contract, Canada will pay the Contractor the firm annual per-Active Audio/Web annual license fee identified by the per Active User Audio/Web annual license fee from the applicable range of Active User count, set out in Annex E multiplied by the number of Active Users, on the anniversary date of the In-Service date, Applicable Taxes extra.

7.11.1.4 **Milestone Payment for Portal Services**: For completing the gates of the portal development and implementation for the COAS services in accordance with the Contract, upon approval by Technical Authority, Canada will pay the Contractor the firm price per milestone, set out in Annex E, applicable Taxes extra.

7.11.1.5 **Competitive Award**: The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

7.11.1.6 **Travel and Living Expenses:** Canada will not pay any travel and living expenses associated with the performance of the Work.

7.11.1.7 **Service Catalogue:** The Parties agree that the prices set out in Annex E: (or referred to as Service Catalogue) represent the complete prices chargeable by the Contractor for providing all of the services described in the Statement of Work (including all labour, equipment, parts, infrastructure, overhead and any other costs associated with implementing and providing the services), except where the Contract expressly refers to prices to be negotiated on a case-by-case basis or where otherwise noted. The Contractor must not add any other charges of any type or for any reason to invoices rendered under this Contract.

7.11.1.8 **Purpose of Estimates**: All estimated costs contained in the Contract are included solely for the administrative purposes of Canada and do not represent a commitment on the part of Canada to purchase goods or services in these amounts. Any commitment to purchase specific amounts or values of goods or services is described elsewhere in the Contract.

7.11.2 **Monthly Payment:** H1008C (bearing the most recent date on or before the date this contract was issued), Monthly Payment

7.11.2.1 Canada will pay the Contractor on a monthly basis, for per minute and per flat rate fee services, in accordance with Annex E, consumed in the previous month covered by the invoice in accordance with the payment provisions of the Contract if:

7.11.2.1.1 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;

7.11.2.1.2 all such documents have been verified by Canada; and

7.11.2.1.3 the Work performed has been accepted by Canada.

7.11.3 **Milestone Payment – Not subject to holdback:** H3010C (bearing the most recent date on or before the date this contract was issued),

7.11.3.1 Canada will pay the Contractor on a milestone basis, for each gate of the portal development and implementation as described in the Statement of Work, Annex A, and in accordance with the firm price per milestone in Annex E, in accordance with the payment provisions of the Contract if:

7.11.3.1.1 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;

7.11.3.1.2 all such documents have been verified by the Technical Authority; and

7.11.3.1.3 the Work performed has been accepted by the Technical Authority.

7.11.4 **Advance Payment:** H3028C (bearing the most recent date on or before the date this contract was issued),

7.11.4.1 For Per Active User Audio/Web Annual Licenses, Canada will pay the Contractor in advance, on an annual basis, on the anniversary date of the Contract In-Service for the number of Active User licenses for the following year as identified by SSC; if

7.11.4.1.1 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 and all such documents have been verified by Canada, and;

7.11.4.1.2 The number of Active User Audio/Web annual licenses billed is in accordance with the number of Active Users identified by SSC as described in the Statement of Work, Annex B.

7.11.5 **Amending the Service Catalogue**

7.11.5.1 The prices set out in the Service Catalogue represent firm unit prices for the duration of the Contract Period, including the option years. The Contractor cannot increase any price, however; the Contractor may, at any time, reduce the price for one or more Services identified in the Service Catalogue by sending written notice to the Contracting Authority, who will issue an amendment.

7.11.5.2 Any price adjustment pursuant to this Article will be effective immediately upon receipt by Canada of the written notice from the Contractor; provided, however, the Contractor may specify that a price adjustment will be effective on the first day of its next billing cycle.

7.11.5.3 The Service Catalogue can be amended by the Contracting Authority, following written agreement between Canada and the Contractor to include any new feature, functionality, or service offering, within the scope of the COAS.

7.11.6 **Prices to be Negotiated**

7.11.6.1 For all items for which the Contract expressly refers to pricing being negotiated (for example, for services added to the Contract pursuant to the Sub-article further above entitled "Service Evolution"), upon request by the Contracting Authority, the Contractor must submit one or more (as requested) of the following forms of price support for the prices it proposes:

7.11.6.1.1 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);

7.11.6.1.2 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; and

7.11.6.1.3 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, markup, etc.; and/or a price certification from the Contractor.

7.12 Remedies and Service Credits

7.12.1 **Service Credits Apply during Entire Contract Period:** The Parties agree that the remedies and Service Credits apply throughout the Contract Period, including during implementation.

7.12.2 **Service Credits represent Liquidated Damages:** The Parties agree that the Service Credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

7.12.3 **Payment of Service Credits:**

7.12.3.1 If the Contractor fails to meet the Service Level Targets set out in Annex A: Statement of Work General, the Contractor must pay to Canada the associated liquidated damages (referred to as "Service Credits").

7.12.3.2 To collect the Service Credits, Canada has the right to hold back, drawback, deduct or set off from and against any money Canada owes to the Contractor from time to time. When amounts are due to Canada with respect to Service Credits, Canada reserves the right to require a payment:

7.12.3.2.1 by way of a credit against the price payable pursuant to this Contract; or

7.12.3.2.2 by way of a credit against the price payable pursuant to another contract between the Parties.

7.12.3.3 For any given month, Canada agrees first to exhaust the Service Credits against the price payable pursuant to this Contract under (a), before exercising its rights pursuant to (b).

7.12.3.4 The Contractor must convert Service Credits to Canadian dollars using the exchange rate established by the Bank of Canada at the beginning of the month for the country and in the month where the Service Credits were incurred.

7.12.4 **Credits for Failure to Complete Each SA&A Gate:**

7.12.4.1 If the Contractor does not receive acceptance or conditional acceptance for each of the SA&A Gate 1, 2, and SA&A In-Service deliverables in accordance with the timeframe in Table entitled Project Milestones in the Statement of Work, Annex A, the Contractor must provide a credit to Canada in the amount of $20,000 and an additional $2,000 for each FGWD thereafter that acceptance or conditional acceptance is not received.

7.12.4.2 If Canada grants conditional acceptance to the Contractor for any SA&A Gate deliverable and the Contractor fails to obtain Canada's acceptance of the SA&A Gate deliverable by the approved new deadline, the conditional acceptance for the SA&A Gate deliverable will automatically be revoked. In that case, the Service Credit that applies for failure to complete the SA&A Gate deliverable on the new schedule will apply.

7.12.4.3 In cases where Canada delays approval for SA&A Gates 1, 2 and SA&A In-Service deliverables, the Contracting Authority reserves the right to extend the timelines for SA&A Gates 1, 2 and SA&A In-Service in the Table entitled Project Milestones.

7.12.5 **Credits for Failure to Deliver Operational Service Portal:**

7.12.5.1 If the Contractor does not receive acceptance or conditional acceptance for the Service Portal Gates 1, 2, 3 and Service Portal In-Service deliverables in accordance with the timeframe in Table entitled Project Milestones in the Statement of Work, Annex A, the Contractor must provide a credit to Canada in the amount of $30,000 and an additional $2,000 for each FGWD thereafter that acceptance or conditional acceptance is not received.

7.12.5.2 If Canada grants conditional acceptance to the Contractor for the delivery of the operational Service Portal and the Contractor fails to obtain Canada's acceptance by the approved new deadline, the conditional acceptance for Service Portal will automatically be revoked. In that case, the Service Credit that applies for failure to complete the Service Portal on the new schedule will apply.

7.12.5.3 In cases where Canada delays approval for Service Portal Gates 1, 2, 3 and Service Portal In-Service deliverables, the Contracting Authority reserves the right to extend the timelines for Gates 1, 2, 3 and SA&A In-Service in the Table entitled Project Milestones in the Statement of Work, Annex A.

7.12.6 **Failure to Deliver COAS Services**

7.12.6.1 If the Contractor fails to obtain Canada's acceptance of the Work identified for COAS Services Gate 1 and COAS In-Service in accordance with the timeframe in Table entitled Project Milestones in the Statement of Work, Annex A, the Contractor must provide a credit to Canada in the amount of $5,000 for each FGWD that acceptance or conditional acceptance is not received.

7.12.6.2 If the required Work for Operational Readiness has still not been completed and accepted within 145 FGWDs after Contract Award, subject to Excusable Delay, the Parties agree that this constitutes a fundamental breach of the Contract and that Canada may terminate the Contract for default, without providing any further notice or opportunity to cure. The Parties further agree that these are not the only circumstances in which the Contract can be terminated for default, as this clause does not detract from or alter Canada's rights pursuant to Section 29 of General Conditions 2035.

7.12.7 **Failure to Meet Service Level Target for Maximum Time to Restore the COAS Service, or any portion of the Service (SLT-MTTR-COAS)**

7.12.7.1 Commencing on the In-Service date, if the Contractor fails to meet SLT-MTTR-COAS as per the Statement of Work, Annex A, then the Contractor must provide a Service Credit to Canada for:

7.12.7.1.1 first occurrence in any 12-month period is $5,000 and $1,000 for each additional 30 minutes or part thereof;

7.12.7.1.2 second occurrence in any 12-month period is $10,000 and $1,000 for each additional 30 minutes or part thereof; and

7.12.7.1.3 third and subsequent occurrences in any 12-month period is $15,000 and $1,000 for each additional 30 minutes or part thereof.

7.12.8 **Failure to Meet Service Level Target for Service Portal Maximum Time to Restore (SLT-SP-MTTR)**

7.12.8.1 Commencing on the In-Service date, if the Contractor fails to meet SLT-SP-MTTR as per the Statement of Work, Annex A then the Contractor must provide a Service Credit to Canada of $10,000. For each additional 30.0 minutes of Service Portal outage time, the Contractor must provide Canada with an additional Service Credit of $1,000.

7.12.8.2 If the Contractor fails to meet the SLT-SP-MTTR three or more times in any 12-month period, the Service Credit payable to Canada for the third and each subsequent individual occurrence in the same 12-month period will automatically double.

7.12.9 **Failure to Meet Service Level Target for Billing Format and Timing (SLT-BF-T)**

7.12.9.1 Commencing on the In-Service date, each month that the Contractor fails to deliver accurate billing files within 10 FGWD's following the end of the previous month as per the Statement of Work, Annex A, the Contractor must provide a credit to SSC of $1000.00 for each day starting on the due date based on the following:

7.12.9.1.1 SSC will open an Incident for incorrect EBDF formatting, the Contractor must correct the formatting and reissue the EBDF within 2 FGWDs.

7.12.9.1.2 SSC will open an Incident for a late EBDF, the Contractor must issue the EBDF within 1 FGWD.

7.12.10 **Corrective Measures**:

7.12.10.1 If credits are payable under this Article for two consecutive months or for three months in any 12-month period, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Contracting Authority and 20 working days to rectify the underlying problem.

7.12.11 **Contractor Failure to Perform its Responsibilities**

7.12.11.1 The process for requiring the Contractor to undertake remedial action if the Contractor fails to meet the Work responsibilities defined in the Contract will be as follows:

7.12.11.1.1 Canada will notify the Contractor in writing (e.g., email) that a failure to meet a Work responsibility has occurred. Canada will provide specific details regarding the failure.

7.12.11.1.2 The Contractor must respond to Canada within 3 FGWDs with an action plan to resolve the failure for Canada's approval. The Contractor's action plan must demonstrate how the failure will be resolved within 20 FGWDs of the notification from Canada including Canada's time for review and approval of the action plan.

7.12.11.1.3 Canada will provide a response to an action plan submitted by the Contractor (approved, rejected with disposition) within 2 FGWDs of receiving the action plan. Where Canada requires more time than the 2 FGWD review period, the time to resolve the failure will be increased by the additional FGWDs beyond the 2 FGWD review period.

7.12.11.1.4 If the Contractor fails to deliver an action plan, or if in Canada's opinion the Contractor has failed to resolve the failure according to the approved action plan within the 20 FGWD period, then the Contractor must provide Canada with a Service Credit of $1,000 for each FGWD or partial FGWD the failure is not resolved beyond the 20 FGWD period.

7.12.11.1.5 Where there is already a remedial action applied for failure to complete Work, the Contractor must provide a Service Credit of $1,000 (as per preceding sub-paragraph) or the Service Credit for the other remedial action, whichever is greater, as calculated for the duration of the Service Credit activity.

7.12.12 **Service Credit Calculation**

7.12.12.1 The Contractor must calculate Service Credits based on its performance of the Work against the Service Level Targets for the previous month beginning on the first day of each monthly billing cycle and ending on the last day of that billing cycle.

7.12.13 **Termination for Failure to Meet Service Level Targets**

7.12.13.1 In addition to any other rights it has under the Contract, Canada may terminate the Contract for default in accordance with the General Conditions (except there will be no opportunity to cure), if over the course of any 12-month period, there are two months in which, if the Service Credit Cap did not apply, the total amount of Service Credits for that monthly billing cycle would have been 25% or more of the amount that would have been payable to the Contractor for that month (not including applicable taxes) for all Services if no liquidated damages had accrued.

7.12.14 **Canada's Rights & Remedies not Limited**:

7.12.14.1 The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

7.12.15 **Discretionary Audit – Commercial Goods and /or Services**:

7.12.15.1 The Contractor certifies that the price or rate is not in excess of the Contractor's published commercial pricing for like services. This is subject to verification by government audit, at the discretion of Canada, before or after payment is made to the Contractor.

7.12.15.2 The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately credited to Canada in the Contractor's invoices.

7.12.15.3 The Contractor agrees that any comparison or consideration of like services:

7.12.15.3.1 Excludes customization or special items, as these should be priced separately; and

7.12.15.3.2 Excludes costs related to matters such as billing (e.g., consolidated invoice requirements), administration, registration in SSC's P2P Portal, or submission of information, as these are the Contractor's typical costs of doing business.

7.12.15.4 If the audit demonstrates that the pricing is in excess of the Contractor's published commercial pricing for like services before and/or after payment is made, the Contractor agrees that future invoices will be adjusted by Canada in accordance with the results of the audit. It is further agreed that if the Contract is still in effect at the time of the verification, the price or rate will be lowered in accordance with the result of the audit.

7.12.15.5 If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year).

7.12.15.6 If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

7.13 Limitation of Expenditure

7.13.1 Canada's total liability to the Contractor under the Contract must not exceed the amount set out on page 1 of the Contract. With respect to the amount set out on page 1 of the Contract, Customs duties are excluded and Applicable Taxes are included, if applicable. Any commitments to purchase specific amounts or values of goods or services are described elsewhere in the Contract.

7.13.2 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 Contracting 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 Contracting Authority.

7.13.3 The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum when:

7.13.3.1 it is 75 percent committed, or

7.13.3.2 4 months before the Contract expiry date, or

7.13.3.3 as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

7.13.4 If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Providing this information does not increase Canada's liability.

7.14 Invoicing

7.14.1 The Contractor must, monthly, submit an SSC Summary Invoice and Client Summary Invoices in accordance with the information required in the General Conditions, and in the Statement of Work, Annex A.

7.14.2 The Contractor's Invoices must be submitted in the Contractor's own form, which must include the Contractor's official letterhead or logo and the Contract number.

7.14.3 The Contractor's Monthly Service charges on the monthly EBDF must include all charges (i.e. AWCS Services, OAS Services, service credits, milestone payments, CR costs, etc.) and must match the total of the:

7.14.3.1 Client Summary Invoices; and

7.14.3.2 SSC Summary Invoice.

7.14.4 By submitting Monthly Invoices, the Contractor is certifying the Services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, Statements of Work, Annexes A, B, C and Annex E – Pricing Table, Change Request(s) and Service Credits when applicable, including any charges for work performed by subcontractors.

7.14.5 The Contractor must provide Invoices that cover Services delivered from the first day of the calendar month until the last day of the calendar month. Invoice must include all charges for this billing period and must include a separate line item for:

7.14.5.1 previous balance;

7.14.5.2 billing adjustments (from previous periods);

7.14.5.3 payments made;

7.14.5.4 outstanding balance;

7.14.5.5 AWCS Services;

7.14.5.6 OAS Services;

7.14.5.7 Service Portal;

7.14.5.8 service credits;

7.14.5.9 other charges and credits;

7.14.5.10 taxes; and

7.14.5.11 balance due.

7.14.6 Unless requested to do otherwise by the Contracting Authority, the Contractor must invoice each Client directly according to the Subscriber's User profile.

7.14.7 Unless requested to do otherwise by the Contracting Authority, the Contractor must invoice SSC for all Partners and SSC itself directly according to the Subscriber's User profile.

7.14.8 The Contractor must provide an electronic copy of all Summary Invoices (i.e. per Client and SSC including Partners) in Portable Document Format (PDF) uploaded to the Document Management System (DMS) and emailed to each Client's billing email address. If billing email address is not available a hardcopy must be sent to the Client's billing address.

7.14.9 In addition to the Monthly Summary Invoices, the Contractor must submit a monthly EBDF as per Appendix 2 to Annex A – Electronic Billing Detail File format.

7.14.10 The Contractor must acknowledge that the monthly EBDF will be validated automatically through an SSC application for the relevant billing period. Charges for all services must match those in the Annex E – Pricing Table, and Change Request(s), when applicable, or line items could be rejected individually based on contracted rates. If a charge is rejected, SSC will advise the Contractor of the reason for the rejection, and SSC will create a file and/or report on behalf of itself and it's Clients that will be sent back to the Contractor for correction in the next month's billing cycle. SSC and Clients will pay the total amounts of the Summary Invoices to the Contractor. The Contractor must make the billing adjustments on the next month's EBDF and Monthly Summary invoices for the billing files to be 100% accurate.

7.14.11 The Contractor must provide a designated technical billing resource, available to assist the Technical Authority with the monthly reconciliation of any billing exceptions, errors, or credits.

7.14.12 The Contractor must provide a Billing Escalation Matrix, within 20 FGWDs' of Contract award, with the names of personnel for a minimum of 4 levels of escalation (from Escalation Level 1 to Escalation Level 4 as the most senior personnel, with corresponding authority levels in the Contractor's and SSC's organizations, as in sample below:

Escalation Levels	**Name of SSC Person to Contact SSC - Escalation if necessary**	**Name of Contractor Person to Contact Contractor - Escalation if necessary**

1	e.g. Name of SSC Billing Resource	e.g. Name of Contractor Billing/Service Management
2	e.g. Name of Manager – Billing/Service Management	e.g. Name of Manager Billing/Service Management
3	e.g. Name of Director – Billing/Service Management	e.g. Name of Director - Billing/Service Management
4	e.g. Name of DG – Billing/Service Management	e.g. Name of VP - Billing/Service Management

7.14.13 The Contractor must reverse any rejected charges in the subsequent billing cycle and has a maximum of up to 3 billing periods in which to correct the billing charges. The Contractor must not submit any charges older than four months; if the Contractor does so, Canada has no obligation to pay for those charges.

7.15 Acceptance Procedures for Service Portal and SA&A

7.15.1 **Scope of the process:** The process described in this Article applies to the **acceptance** of the work completed by the Contractor with the exception of work to fulfill Service Requests. The process for acceptance of work for In-Service Requests and Reservations is defined in the Statement of Work, Annex A.

7.15.2 **Acceptance of work:** The Contractor's work is only considered to be completed after it has received the Technical Authority's formal written acceptance.

7.15.3 **Time for Canada's review and acceptance process:** The Contractor must seek and obtain Canada's acceptance or conditional acceptance for all deliverables as described in Statement of Work, Annex A, Section 5 – Operational Readiness, and in accordance with the delivery timeframes. The Contractor must include time for Canada's review and acceptance process, including any meetings, within the work delivery timeframe requirements specified in the Contract.

7.15.4 **Meetings:** Canada may request meetings with the Contractor during its review period, and the Contractor may request meetings with Canada following receipt of Canada's notice of any deficiencies. Canada will meet with the Contractor within 2 FGWDs of the Contractor's request following Canada's rejection of a deliverable. The Contractor must meet with Canada within 2 FGWDs of Canada's request.

7.15.4.1 For example, if the Contractor is required to provide the SRS for the Service Portal within 40 FGWDs of Contract award, the Contractor must factor Canada's review of that deliverable, and any subsequent meetings that might be required if there are deficiencies, within that schedule.

7.15.5 **No additional time to remedy deficiencies:** Canada is not required to provide additional time to the Contractor if Canada determines that the Contractor's work is deficient and Canada does not provide acceptance.

7.15.6 **Acceptance form:** Within 10 FGWDs of Contract award, the Contractor must develop an acceptance form to be used to obtain written acceptance from Canada for the Contractor's work requiring acceptance. The acceptance form must, at a minimum, include fields and/or tables for:

7.15.6.1 tracking iterations;

7.15.6.2 a description of the project deliverable;

7.15.6.3 the required completion date for the deliverable according to the approved Implementation Plan and Implementation Plan version;

7.15.6.4 the date the deliverable is submitted to Canada for review and acceptance;

7.15.6.5 the name, date and signature of the Contractor's Project Manager that has reviewed and endorses the quality and completeness of the work being submitted for acceptance;

7.15.6.6 check-boxes for Canada to indicate acceptance or rejection of the work being submitted for acceptance;

7.15.6.7 Canada to enter the reason for rejecting the work being submitted for acceptance;

7.15.6.8 the name, date and signature of Canada's Technical Authority;

7.15.6.9 the date that Canada responds with acceptance or rejection of the work being submitted for acceptance;

7.15.6.10 the date that Canada meets with the Contractor (at the Contractor's request) to review the work being submitted for acceptance; and

7.15.6.11 the number of FGWDs that the delivery timeframe for the work being submitted for acceptance is extended due to Canada's delay (beyond the specified number of FGWDs) in its review, or delay (beyond the specified number of FGWDs) in meeting with the Contractor to discuss concerns about a deliverable.

7.15.7 **Extensions:** Canada may, in its sole discretion, agree in writing to extend the delivery timeframes for a deliverable, and thereby extend the date by which the Contractor must obtain Canada's acceptance, for any aspect of the work associated with the deliverable. However, any such individual extension does not, in itself, extend the deadline for any other deliverable. If Canada provides an extension for a specific deliverable, the extension will only apply to that deliverable and not to any other deliverable. For the deliverables for which any extension has been granted, the Contractor must obtain Canada's acceptance by the extended deadline approved by Canada for each deliverable.

7.15.8 **Extensions relating to SA&A:** With regard to the delivery timeframes associated with Security Assessment and Authorization (SA&A), any delay (i.e., beyond 5 FGWDs) in Canada's review and response to Gate 1 deliverables will extend the date for the completion of Gate 2. Any delay in Canada's review and response for Gate 2 deliverables will similarly extend the SA&A In-Service date.

7.15.9 **Approval Escalation Process:**

7.15.9.1 The Contractor must work co-operatively with SSC to comply with each Security Requirement (SR) for the completion of the SA&A process.

7.15.9.2 The Contractor must work with SSC to resolve any problems and issues quickly and effectively, by prompt response times and resolution.

7.15.9.3 The Contractor must immediately escalate the resolution of problems and issues to a higher authority if the problem remains unresolved, and escalation is requested by the SSC representative assessing the SRTM(s).

7.15.9.4 The Contractor must include in its Escalation Matrix the personnel, and must include a minimum of 4 levels of escalation (from Escalation Level 1 to Escalation Level 4 as the most senior personnel, with corresponding authority levels in the Contractor's and SSC's organizations, as in sample below.

7.15.9.5 During the Project Kick-Off Meeting, the Technical Authority will provide SSC's escalation contacts and alternates to the Contractor, as in sample below.

Escalation Levels	Name of SSC Person to Contact for Escalation if necessary	Name of Contractor Person to Contact for Escalation if necessary

1	e.g. Name of Security Assessor	e.g. Name of Security Assessor
2	e.g. Name of Manager of Security	e.g. Name of Manager of Security
3	e.g. Name of Director of Security	e.g. Name of Director of Security
4	e.g. Name of VP of Security	e.g. Name of VP of Security

7.15.9.6 Within 15 FGWDs from Contract Award, and whenever the Escalation Matrix is updated, the Contractor must advise the TA and upload to the DMS. This procedure must be consistent with the Contractor's obligations under the Contract and must be approved by the Technical Authority.

7.15.9.7 The Contractor must provide SSC with notification of issues according to the Escalation Matrix .

7.15.9.8 The Contractor must change the Escalation Level for issues within 1 hour of a request by SSC.

7.15.9.9 The Contractor must automatically provide escalation information by email to escalation contract specified by SSC in the escalation matrix until the issue is resolved.

7.15.10 **Acceptance of SA&A deliverables**:

7.15.10.1 The Contractor must submit all deliverables for the work to the Technical Authority by email, and also notify the Contract Authority using email.

7.15.10.2 Canada's acceptance process will begin from the time and date that the email is received by the Technical Authority containing the:

7.15.10.2.1 acceptance form for the deliverable; and

7.15.10.2.2 deliverable in a format specified by Canada;

7.15.10.3 Canada will provide a written response to the Contractor within 5 FGWDs that will indicate either acceptance of the work or will describe any deficiencies that the Contractor must correct in order to obtain Canada's acceptance.

7.15.10.4 If Canada does not provide a written response within 5 FGWDs, or Canada is unable to meet with the Contractor within 2 FGWDs of a request for review of a deliverable, the Contractor's required delivery timeframe specified in the Contract will automatically be extended by the same number of FGWDs that Canada delayed its response beyond the 5 FGWDs, or delayed meeting with the Contractor beyond 2 FGWDs.

7.15.11 **Acceptance of Operational Service Portal**:

7.15.11.1 An acceptance form must be received by the TA for the Service Portal Gate 1, Gate 2, 3 and Service Portal In-Service Milestone deliverables. The TA can provide approval, interim approval (with deficiencies and dates for remediation) or reject approval (with deficiencies). If Canada does not approve, the Contractor must address the deficiency at no cost within the dates for remediation to Canada as soon as possible and notify Canada in writing once the deficiencies are corrected and re-issue the acceptance form, at which time Canada will be entitled to re-inspect the work.

7.15.12 **Acceptance of COAS Services**:

7.15.12.1 An acceptance form must be received by the TA for the COAS Services Gate 1 and COAS Services In-Service Milestone deliverables. The TA can provide approval, interim approval (with deficiencies and dates for remediation) or reject approval (with deficiencies). If Canada does not approve, the Contractor must

address the deficiency at no cost within the dates for remediation to Canada as soon as possible and notify Canada in writing once the deficiencies are corrected and re-issue the acceptance form, at which time Canada will be entitled to re-inspect the work.

7.15.13 **Conditional Acceptance**:

7.15.13.1 Canada may, in its sole discretion, agree in writing to accept a deliverable relating to the Service Portal or relating to SA&A on a conditional basis. Conditional acceptance for any given deliverable means that Canada accepts it, subject to specific items that require correction in order to provide final acceptance. Where Canada conditionally accepts a deliverable, Canada will identify to the Contractor the remaining work that must be completed for the deliverable to receive Canada's final acceptance and the deadline for final acceptance, which includes any time required by Canada to review that work. Canada's conditional acceptance of any such deliverable allows the Contractor to move on with any part of the work that was otherwise contingent on acceptance of that deliverable. Canada's conditional acceptance of any such deliverable also has the effect of suspending any Service Credits that would apply for late delivery of that deliverable. However, if a deliverable that has been conditionally accepted by Canada does not receive final acceptance in accordance with the new deadline established by Canada for that deliverable, any Service Credits will apply retroactively to the initial date on which the deliverable was due.

For example, Canada agrees to extend the deadline for acceptance of the Service Design for 20 FGWDs beyond the originally scheduled completion date.

If the Contractor does not obtain Canada's acceptance for the Service Design within the 20 FGWDs, Service Credits will apply, counted from the original deadline for acceptance of the Service Design (i.e., counted from 20 FGWDs after Contract award).

7.15.14 **Compliance with Certifications:** Compliance with the certifications provided by the Contractor in its bid is a condition of the Contract and subject to verification by Canada during the entire Contract Period. The Contracting Authority may ask for additional information to verify the Contractor's certifications at any time during the Contract Period. If the Contractor does not provide the requested additional information or does not comply with any certification or it is determined that any certification made by the Contractor in its bid is untrue, regardless of whether or not the Contractor knew when it made the certification that it was untrue, and regardless of whether or not the certification became untrue after it was made, Canada has the right to terminate the Contract for default.

7.16 Federal Contractors Program for Employment Equity – Default by the Contractor

7.16.1 The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire Contract Period. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.17 Foreign Nationals (Canadian Contractor)

7.17.1 SACC Manual clause A2000C (2006-06-16) Foreign Nationals (Canadian Contractor)

7.18 Applicable Laws

7.18.1 The Parties agree that this Contract will be interpreted and governed, and the relations between the Parties determined, by the laws in force in the Province of Ontario. The Parties further agree that any disputes relating to the Contract will be determined in accordance with the laws of, and by the courts of, the Province of Ontario.

7.19 Priority of Documents

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

7.19.1.1 Section 02 of Supplemental General Conditions 4005 (Telecommunications Services and Products) entitled "Termination Rights Associated with Breach of Telecommunications Warranties and Representations";

7.19.1.2 _____ (collectively referred to as the "**Tariff**")

Note to Bidders: This clause will not be included in any resulting contract if the Contractor's bid is not subject to any tariffs.

7.19.1.3 These Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;

7.19.1.4 supplemental general conditions, in the following order:

7.19.1.4.1 4005; other than Section 02, which takes priority as set out above under sub-paragraph 5.10.1.1

7.19.1.4.2 4006;

7.19.1.5 General Conditions 2035;

7.19.1.6 Annex A, Conferencing & Operator Assisted Services – General SOW;

7.19.1.7 Annex B, Conferencing & Operator Assisted Services – Audio/Web SOW;

7.19.1.8 Annex C, Conferencing & Operator Assisted Services – OAS SOW;

7.19.1.9 Annex D, Security Requirements Check List (SRCL);

7.19.1.10 Annex E, Pricing Table (Service Catalogue);

7.19.1.11 Annex F, COAS CSP Security Obligations;

7.19.1.12 Annex G, SCSI Submission Form;

7.19.1.13 Appendix 1 to Annexes A, B and C, Glossary;

7.19.1.14 Appendix 2 to Annex A, Electronic Billing File Format;

7.19.1.15 Appendix 3 to Annex A, Security Requirements;

7.19.1.16 Appendix 1 to Annex E, Optional Features and Functions; (for future use, if required)

7.19.1.17 Appendix 1 to Annex G, Supply Chain Security Information Assessment Process;

7.19.1.18 the Contractor's bid dated _____(TO BE INSERTED UPON CONTRACT AWARD), as amended, not including any software publisher license terms and conditions that may be included in the bid, and not including any provisions in the bid with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the bid.

7.20 Insurance Requirements

7.20.1 SACC Manual clause G1005C (bearing the most recent on or before the date on contract award) - Insurance Requirement

7.21 Limitation of Liability

7.21.1 This Article applies despite any other provision of the Contract and replaces the section of the General Conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This Article applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this Article, even if it has been made aware of the potential for those damages.

7.21.2 **First Party Liability**:

7.21.2.1 The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:

7.21.2.1.1 any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";

7.21.2.1.2 physical injury, including death.

7.21.2.2 The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

7.21.2.3 Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

7.21.2.4 The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under subparagraph 7.21.2.1 above.

7.21.2.5 The Contractor is also liable for any other direct damages to Canada caused by the Contractor in any way relating to the Contract including:

7.21.2.5.1 any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

7.21.2.5.2 any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this Sub-article concerning "other direct damages" of 0.25 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the block titled

"Total Estimated Cost") or $2,000,000, whichever is the greater amount.

7.21.2.6 In any case, the total liability of the Contractor under this Sub-article 7.21.2.5 2) will not exceed the total estimated cost (as defined above) for the Contract. [*Note to Bidders: The cross-references will be updated at the time of Contract award, since the Contract will no longer be Part 5 in a larger document.*]

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

7.21.3 **Third Party Claims**:

7.21.3.1 The Parties are only liable to one another for damages to third parties to the extent described here:

7.21.3.1.1 Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

7.21.3.1.2 If Canada is required, as a result of joint and several liability, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite Sub-article 7.21.3.1, with respect to special, indirect, and consequential damages of third parties covered by this Section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

7.22 Process for Ordering Services

7.22.1 **Provision of Services**: Whenever it receives a Service Request or Reservation from a Subscriber, the Contractor agrees to provide the ordered Audio/Web and Operator-Assisted Conferencing services in accordance with the terms and conditions and at the prices set out in the Contract (the "**Services**"). Regardless of when a Service Request or Reservation is issued, all Service Requests and Reservations automatically end on the last day of the Contract Period, and Canada is not required to cancel any Service Request at the end of the Contract Period.

7.22.2 **Delivery Date**: The Contractor must deliver the Services within the time period(s) identified in the **Service** Requests and Reservations.

7.23 Access to Canada's Property and Facilities

7.23.1 Canada's property, facilities, equipment, documentation, and personnel are not automatically available to the Contractor. If the Contractor would like access to any of these, it is responsible for making a request to the Technical Authority. Unless expressly stated in the Contract, Canada has no obligation to provide any of these to the Contractor. If Canada chooses, in its discretion, to make its property, facilities, equipment, documentation or personnel available to the Contractor to perform the Work, Canada may require an adjustment to the Basis of Payment and additional security requirements may apply.

7.24 Safeguarding Personal Information

7.24.1 To the extent any Personal Information is stored on Contractor systems or the Contractor is required to handle (collect, retain, use, disclose and dispose) any Personal Information or records, the Contractor must safeguard the Personal Information at all times by taking all administrative, physical and technical security measures that are necessary to secure and protect its availability, integrity and confidentiality. Such measures must be approved by Canada. To do so, at a minimum, the Contractor must:

7.24.1.1 store the Personal Information electronically and implement adequate access controls for access to the system or database in which the Personal Information is stored in accordance with the Security Requirements defined in this Contract;

7.24.1.2 restrict access to the Personal Information and the Records by ensuring that passwords or other access controls are provided only to individuals who require access to the Personal Information in order to perform the Work;

7.24.1.3 ensure that employees who have access to the system have been granted the appropriate security clearance as specified by Canada in accordance with **Error! Reference source not found.Error! Reference source not found.**;

7.24.1.4 safeguard the Personal Information transmitted, processed, or stored by the Contractor in a manner appropriate for the sensitivity of the Personal Information;

7.24.1.5 implement any reasonable security or protection measures requested by Canada from time to time, as a Change Request (CR), as appropriate; and

7.24.1.6 notify the Contracting Authority immediately of any privacy and security breaches; for example, any time an unauthorized individual accesses any Personal Information.

7.24.2 The Contractor's obligations to protect Personal Information shall continue even after the completion or termination of the Contract to the extent required by law.

7.24.3 The Contractor must provide a list of all locations where hard copies of Personal Information are stored.

7.24.4 Upon request, the Contractor must provide a list of every person to whom the Contractor has granted access to the Personal Information or the Records as well as their security clearance level.

7.25 Data Ownership & Sovereignty

7.25.1 Canada does not grant to the Contractor any rights and access to COAS Data at any time. Services are intended only to transport, process and store COAS Data. Furthermore, the

Contractor agrees that it is strictly prohibited from accessing COAS Data, or permitting any third party to access COAS Data, at any time, except with the written consent of the Technical Authority or Contract Authority.

7.25.2 The Contractor acknowledges that Canada Data includes confidential and sensitive information, including, without limitation, confidential and trade secrets of third parties, personal and private information of individuals, confidential information, classified and protected information, and other sensitive information and that a third party accessing Canada Data could affect, among other things, Canada's national interest and national security.

7.25.3 Throughout the Contract Period, the Contractor must implement and follow processes and controls that preserve the integrity, confidentiality and accuracy of all information and data and metadata, irrespective of format. This applies to all information, data and metadata in the Contractor's possession or under its care or control if the information, data or metadata is generated by, acquired pursuant to, or arises in any other way out of the Contractor's responsibilities and obligations under the Contract. The Contractor acknowledges that this is required in order to ensure that Canada can rely on the information, data and metadata and so that Canada can meet its own legal obligations, including statutory obligations. This is also required to ensure the information, data and metadata can be used as persuasive evidence in a court of law.

7.25.4 The Contractor must, to the full extent it is permitted by law, fully cooperate with Canada and assist Canada in responding to access to information requests, investigating complaints, investigating regulatory or criminal matters and prosecutions. This includes allowing Canada to conduct security audits/inspections and furnishing Canada with such information (e.g., documentation, data protection description, data architecture and security descriptions) as may be required by Canada within 5 FGWDs of a request by Canada.

7.25.5 Despite any section of the General Conditions relating to subcontracting, the Contractor must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the Contract unless Canada first consents in writing.

7.26 Reporting Requirements

7.26.1 The Contractor must provide the reports in accordance with the format, within the required time periods and using the medium detailed in Annex A, the General Statement of Work for the Conferencing and Operator Assisted Services (COAS).

7.27 Communications Approval

7.27.1 Except for information that the Contractor is required to make available under securities legislation or regulations, the Contractor must obtain the Contracting Authority's approval prior to releasing any public statement related to the award of the Contract. At the Contracting Authority's request, the Contractor must provide a draft of the announcement for SSC review and approval.

7.28 Representations and Warranties

7.28.1 The Contractor made statements regarding its experience and expertise in its bid that resulted in the award of the Contract. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract. The Contractor also represents and warrants that it has, and all its resources and subcontractors that perform the Work have, and at all times during the

Contract Period they will have, the skills, qualifications, expertise and experience necessary to perform and manage the Work in accordance with the Contract, and that the Contractor (and any resources or subcontractors it uses) has previously performed similar services for other customers.

7.28.2 The Contractor represents and warrants that, in addition to meeting the requirements of this Contract, it will provide the Services in a manner consistent with general industry standards reasonably applicable to the provision of such Services. To the extent that the delivery of Service does not perform in accordance with the Contract under normal use and circumstances, the Contractor agrees to make whatever adjustments are required for the Services to perform in accordance with the Contract within 20 FGWDs.

7.29 On-golng Supply Chain Integrity Process

7.29.1 Supply **Chain Integrity Process:** The Parties acknowledge that a Supply Chain Integrity Process assessment was a key component of the procurement process that resulted in the award of this Contract. In connection with that assessment process, Canada assessed the Contractor's Supply Chain Security Information (SCSI) without identifying any security concerns. The following SCSI was submitted: *<include all that are applicable>*

7.29.1.1 an IT Product List;

7.29.1.2 a list of subcontractors; and

7.29.1.3 network diagram(s).

This SCSI is included *as* Annex G. The Parties also acknowledge that security is a critical consideration for Canada with respect to this Contract and that on-going assessment of SCSI will be required throughout the Contract Period. This Article governs that process.

7.29.2 **Assessment of New SCSI:** During the Contract Period, the Contractor may need to modify the SCSI information contained in Annex G. In that regard:

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

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

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

7.29.2.4 Canada may use any government resources or consultants to conduct the assessment and may contact third parties to obtain further information. Canada may use any information, whether it is provided by the Contractor or comes from

another source, that Canada considers advisable to conduct a comprehensive assessment of any proposed new SCSI.

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

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

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

7.29.4 **Addressing Security Concerns:**

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

7.29.4.2 At any time during the Contract Period, if Canada notifies the Contractor that, in Canada's opinion, there is a Product that is being used in the Contractor's solution (including use by a subcontractor) that has been assessed as having the potential to compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, then the Contractor must:

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

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

7.29.4.2.3 implement the mitigation plan approved by Canada.

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

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

measures for Canada's consideration. Canada will then make a final determination.

7.29.5 **Cost Implications:**

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

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

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

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

7.29.5.1.4 the normal useful life of the Product;

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

7.29.5.1.6 the normal useful life of the proposed replacement Product;

7.29.5.1.7 the time remaining in the Contract Period;

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

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

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

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

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

7.29.5.2 Additionally, if requested by the Contracting Authority, the Contractor must submit a detailed cost breakdown, once any work to address a security concern identified under this Article has been completed. The cost breakdown must contain an itemized list of all applicable cost elements related to the work required by the Contracting Authority and must be signed and certified as

accurate by the Contractor's most senior financial officer, unless stated otherwise in writing by the Contracting Authority. Canada must consider the supporting information to be sufficiently detailed for each cost element to allow for a complete audit. In no case will any reimbursement of any expenses of the Contractor (or any of its subcontractors) exceed the demonstrated out-of-pocket expenses directly attributable to Canada's requirement to cease deploying or to remove a particular Product or Products.

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

7.29.6 **General:**

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

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

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

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

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

7.30 Subcontracting

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

7.30.1.1 the name of the subcontractor;

7.30.1.2 the portion of the Work to be performed by the subcontractor;

7.30.1.3 the Designated Organization Screening or the Facility Security Clearance (FSC) level of the subcontractor;

7.30.1.4 the date of birth, the full name and the security clearance status of individuals employed by the subcontractor who will require access to Canada's facilities;

7.30.1.5 completed sub-SRCL signed by the Contractor's Company Security Officer for CISD completion; and

7.30.1.6 any other information required by the Contracting Authority.

7.30.2 For the purposes of this Article, a "subcontractor" does not include a supplier who deals with the Contractor at arm's length whose only role is to provide telecommunications or other equipment or software that will be used by the Contractor to provide services, including if the equipment will be installed in the backbone or infrastructure of the Contractor.

7.31 Change of Control

7.31.1 At any time during the Contract Period, if requested by the Contracting Authority, the Contractor must provide to Canada:

7.31.1.1 an organization chart for the Contractor showing all related corporations and partnerships; for the purposes of this Sub-article, a corporation or partnership will be considered related to another entity if:

7.31.1.1.1 they are "related persons" or "affiliated persons" according to the Canada *Income Tax Act*;

7.31.1.1.2 the entities have now or in the two years before the request for the information had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

7.31.1.1.3 the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

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

7.31.1.3 a list of all the Contractor's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the Contractor is a subsidiary, this information must be provided for each parent corporation or parent partnership, up to the ultimate owner; and

7.31.1.4 any other information related to ownership and control that may be requested by Canada.

If requested by the Contracting Authority, the Contractor must provide this information regarding its subcontractors as well. However, if a subcontractor considers this information to be confidential, the Contractor may meet its obligation by having the subcontractor submit the information directly to the Contracting Authority. Regardless of whether the information is submitted by the Contractor or a subcontractor, Canada agrees to handle this information in accordance with Subsection 22(3) of General Conditions 2035 (General

Conditions – Higher Complexity – Services), provided the information has been marked as either confidential or proprietary.

7.31.2 The Contractor must notify the Contracting Authority in writing of:

7.31.2.1 any change of control in the Contractor itself;

7.31.2.2 any change of control in any parent corporation or parent partnership of the Contractor, up to the ultimate owner; and

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

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

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

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

7.31.6 If Canada determines in its sole discretion that a change of control affecting a subcontractor (either in the subcontractor itself or any of its parents, up to the ultimate owner) may be injurious to national security, Canada will notify the Contractor in writing of its determination. Canada will not be required to provide the reasons for its' determination, if Canada determines in its discretion that the disclosure of those reasons could itself be injurious to national security. The Contractor must, within 90 days of receiving Canada's determination, arrange for another subcontractor, acceptable to Canada, to perform the portion of the Work being performed by the existing subcontractor (or the Contractor must perform this portion of the Work itself). If the Contractor fails to do so within this time period, Canada will be entitled to terminate the Contract on a "no-fault" basis by providing notice to the Contractor within 180 days of receiving the original notice from the Contractor regarding the change of control.

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

7.31.8 Despite the foregoing, Canada's right to terminate on a "no-fault" basis will not apply to circumstances in which there is an internal reorganization that does not affect the ownership of the ultimate parent corporation or parent partnership of the Contractor or subcontractor, as the case may be; that is, Canada does not have a right to terminate the

Contract pursuant to this Article where the Contractor or subcontractor continues, at all times, to be controlled, directly or indirectly, by the same ultimate owner. However, in any such case, the notice requirements of this Article still apply.

7.32 Information and Communication Technology (ICT) accessibility requirements

7.32.1 Electronic documents

7.32.1.1 All electronic non-web documents (e.g. PDF, Microsoft Word and PowerPoint) must be in an accessible format conformant to clause 10 of the EN 301 549 (2018) as detailed in the annex entitled "ICT Accessibility Requirements". Electronic documents include but are not limited to:

7.32.1.1.1 Reports

7.32.1.1.2 E-mail communication with SSC employees

7.32.1.1.3 Documentation listed within the Statement of Work

7.32.1.1.4 Ad-hoc documents requested by SSC

7.32.1.2 Where the procurement includes an Annex with a limited set of accessibility requirements, and the supplier's proposed solution includes other ICT elements that are not included in the listed clauses, the supplier will be held to all relevant accessibility requirements of the EN 301 549 (2018) which includes clauses 5 through 13.

7.32.2 Guidance for creating accessible documents

7.32.2.1 For practical guidance on creating accessible documents, refer to these Accessible Document Guides as detailed in the annex entitled "ICT Accessibility Requirements".

7.32.3 Multiple formats

7.32.3.1 Where documents are provided in more than one format (for example a report provided in both PDF and Excel format), at least one of these must be accessible as detailed in the annex entitled "ICT Accessibility Requirements". The accessible version must provide equivalent information to the inaccessible version. A notice must be posted indicating which format is accessible.

7.32.4 Printed documents

7.32.4.1 Printed documents provided to SSC employees must adhere to the relevant requirements of the electronic documents, including but not limited to text contrast and use of colour. For practical guidance, see the below Accessibility guidance for printed documents.

7.32.4.2 These guidelines are based on the "Clear Print accessibility guidelines" developed by the Canadian National Institute for the Blind (CNIB).

7.32.4.2.1 Contrast

7.32.4.2.1.1 Use high-contrast colours for text and background. Good examples are black or dark blue text on a white or yellow background, or white or yellow text on a black or dark blue background.

7.32.4.2.2 Type of Colour

7.32.4.2.2.1 Printed material is most readable in black and white. Restrict coloured text to things such as titles, headlines or highlighted material.

7.32.4.2.3 Point size

7.32.4.2.3.1 Bigger is better. Keep your text large, preferably between 12 and 18 points, depending on the font. (Point size varies among fonts.) People who are visually impaired might be able to read large print, but not very small text.

7.32.4.2.4 Leading

7.32.4.2.4.1 Leading is the space between lines of text and should be at least 25 to 30 per cent greater than the point size. This space lets readers move more easily to the next line of text. Too much leading, however, makes type harder to read. Heavier typefaces will require slightly more leading.

7.32.4.2.5 Font family and font style

7.32.4.2.5.1 Avoid complicated or decorative fonts. Choose standard sans serif fonts with easily recognizable upper—and lower-case characters. Arial and Verdana are good choices.

7.32.4.2.6 Font heaviness

7.32.4.2.6.1 Use fonts with medium heaviness and avoid light type with thin strokes. When emphasizing a word or passage, use a bold or heavy font. Italics or upper-case letters are not recommended.

7.32.4.2.7 Letter spacing

7.32.4.2.7.1 Don't crowd your text: keep a wide space between letters. The spacing default in your Microsoft Word software program should be an appropriate distance.

7.32.4.2.8 Paper finish

7.32.4.2.8.1 Use a matte or non-glossy finish to cut down on glare

7.32.4.2.9 To reduce distractions, avoid using watermarks or complicated background designs

7.32.4.2.10 Clean design and simplicity

7.32.4.2.10.1 Use distinctive colours, sizes and shapes on the covers of materials to make them easier to distinguish.

7.32.4.2.11 To ensure equal access for persons with print disabilities, accessible electronic versions must be available which provide equivalent content to the printed documents. For further guides, resources and tools created by federal public service employees advancing digital accessibility, Supply Arrangement Holders can refer to the following webpage: https://a11y.canada.ca/en/guides/.

7.33 Reporting on Greenhouse Gas (GHG) Emissions Reduction

7.33.1 The Contractor is requested to deliver services to Canada in a way that is consistent with assisting Canada in addressing its commitment to safeguarding our natural environment. The Contractor must provide a report to Canada annually on January 1 of each calendar year for the entire contract period regarding the measures it took during the previous year to assist Canada in achieving this goal.

7.33.2 The Contractor is required to provide a report detailing their level of participation (i.e., greenhouse gas (GHG) emissions reduction target set in-line with the Paris Agreement or net-zero 2050 target set) from either:

7.33.2.1 an independent third party recognized by and acceptable to SSC, including but not limited to the Science-Based Targets Institute; or

7.33.2.2 Environment and Climate Change Canada's Net-Zero Challenge

7.34 Reporting on Indigenous Benefits Plan (IBP)

7.34.1 Over the term of the contract, the IBP is intended to develop long–term, meaningful, lasting, sustainable benefits for Indigenous professionals and Indigenous businesses in the fields of the Telecommunications and various resource categories required for this contract.

7.34.2 The Contractor will complete the Form – Template for Reporting on the Results of the Indigenous Benefits Plan (IBP) and submit it to the Contracting Authority annually on January 1 of each calendar year during the entire contract period.

7.35 Reporting on Socio-Economic Benefits

7.35.1 The Contractor must submit the Socio-Economic Report Form annually on January 1 of each calendar year during the entire contract period to the Contracting Authority. The Contractor agrees that there will be no additional change for these services.

7.36 Electronic Procurements and Payment (EPP) System

7.36.1 SSC is working on an initiative that is expected to provide it with e-functionality from procurement through payment (the "**EPP (P2P) system**"). SSC's suppliers will be required to interface with that functionality.

7.36.2 Because the functionality will not be ready at the time of Contract award, if Canada wishes for the Contractor to interface with the EPP system during the Contract Period, Canada may issue a Change Request regarding the work required for the Contractor to interface with the EPP system. The Contractor's response to Canada's Change Request must include, in addition to identifying the required resources (and the rates applicable pursuant to the Contract), any costs for hardware or software that will be required, including development costs for work to be performed by third parties.

7.36.3 The Parties agree to work cooperatively to determine the work involved and a reasonable ceiling price for that work. If the Parties agree to proceed with that work, Canada will issue a Contract Amendment documenting the ceiling price associated with the work. The Contractor will be required to submit a service design for approval by Canada and the work associated with the development of any EPP system interfaces will be treated as a Service Project.

7.36.4 Canada will pay the Contractor, in arrears, up to the ceiling price established in the contract amendment, for actual time worked and any resulting deliverables in accordance with firm, all-inclusive per diem rates set out in the relevant Contract Amendment, with GST/HST extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday. When submitting its invoices, the Contractor must show the actual time worked by each resource, and/or the amount paid to any subcontractor. With respect to any expenses, the Contractor will be required to demonstrate the out-of-pocket amount spent and will be reimbursed without the addition of any profit or overhead.

7.36.5 Canada acknowledges that, to the extent changes are required to the COAS Contract, the Contractor is under no obligation to complete the work unless the Parties agree.

7.37 General Security Requirements

7.37.1 The Contractor acknowledges that Canada requires, and the Contractor guarantees that, the Services provided in the Contract are and will be the subject of robust, comprehensive security measures that evolve as security threats and technologies evolve, so that the security measures in use are updated throughout the Contract Period, in order to achieve the highest possible levels of data integrity, availability, and confidentiality.

7.38 Safeguarding Electronic Media

7.38.1 Before using them on Canada's equipment or sending them to Canada, the Contractor 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 Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

7.38.2 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 Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.39 Dispute Resolution

7.39.1 Any dispute concerning this Contract that cannot be resolved by discussions or written communications between the Contracting Authority and the Contractor's Representative within 20 FGWDs will be handled by the process described in this Article.

7.39.2 After the 20 FGWD period, either Party may give notice to the other containing a request to negotiate, which must contain a description of the nature of the dispute, any relevant background details, and refer to specific Articles of the Contract that relate to the dispute. The Party receiving the request to negotiate must provide the request to negotiate to a Senior Director (or equivalent). Within 10 FGWDs of receiving a request to negotiate, the receiving Party must respond in writing with its position regarding the nature of the dispute, any additional relevant details and any additional Articles of the Contract that Party considers relevant to the dispute.

7.39.3 If the dispute is not resolved within 10 FGWDs of the response being provided, the Parties agree to refer the matter to a Director General (or equivalent). Within 10 FGWDs of receiving a request to negotiate, the receiving Party must respond in writing with its position regarding the nature of the dispute, any additional relevant details and any additional Articles of the Contract that Party considers relevant to the dispute.

7.39.4 If the dispute is not resolved within 10 FGWDs of the response being provided, the Parties agree to refer the matter to an Assistant Deputy Minister (or equivalent). Within 10 FGWDs of receiving a request to negotiate, the receiving Party must respond in writing with its position regarding the nature of the dispute, any additional relevant details and any additional Articles of the Contract that Party considers relevant to the dispute.

7.39.5 If the dispute is not resolved through these negotiations within a total of 60 FGWDs (including all of the above steps), the Parties agree to consider referring the matter to more senior officials in their respective organizations and/or to consider other appropriate dispute resolution processes before resorting to litigation.

7.39.6 All information exchanged during these negotiations or other dispute resolution processes will be regarded as "without prejudice" communications for the purpose of settlement negotiations and will be treated as confidential by the Parties and their representatives, unless otherwise required by law. However, evidence that is independently admissible or

discoverable will not be rendered inadmissible or non-discoverable by virtue of its use during the negotiations or other alternate dispute resolution process.

7.40 Transition Services at end of Contract Period

7.40.1 The Contractor acknowledges that the nature of the Services provided under the Contract requires continuity and further agrees that, in the period leading up to the end of the Contract Period (or if the Contract is terminated for any reason before the end of the Contract Period), it will make all reasonable efforts to assist Canada in the transition from the Contract to a new contract with another supplier or to Canada itself.

7.40.2 The Contractor, upon receiving notification of a request to transition Services as a result of Contract termination or expiration, must work with Canada to effect a seamless transition of Service to the follow-on contractor or to Canada, whichever will be performing the same or similar work. In doing so, the Contractor agrees to work closely and co-operatively with the follow-on contractor(s) or Canada at no additional cost.

7.40.3 During transition, the Contractor will work with the Client to arrive at a mutually agreeable schedule for transition that may exceed normal contract turnaround time requirements.

7.40.4 During the Contract Period, the Contractor must continue to provide Services until the Contract is terminated following the transition to the follow-on contractor.

7.40.5 The Contractor must request from Canada, not later than 60 FGWDs before the Contract termination date, disposal instructions for COAS data. The Contractor must return COAS data in accordance with the instructions provided by Canada.

7.40.6 The Contractor agrees that there will be no charge for transition Work.

ANNEX A

STATEMENT OF WORK - GENERAL

ANNEX B

STATEMENT OF WORK – AUDIO AND WEB CONFERENCING

ANNEX C

STATEMENT OF WORK – OPERATOR ASSISTED SERVICES

ANNEX D

SECURITY REQUIREMENTS CHECK LIST

(*insert, if applicable*)

ANNEX E

PRICING TABLE (SERVICE CATALOGUE)

ANNEX X (*insert if applicable*)
FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

Remark to Contracting Authority: *Insert for requirements made on behalf of a Department or Agency subject to the FCP, estimated at $1,000,000* ***and above****, Applicable Taxes included: (consult Annex 5.1 of the Supply Manual)(See also Part 5 - Certifications and Part 7 - Resulting Contract Clauses)*

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with such request by Canada will also render the bid non-responsive or will constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit HRSDC-Labour's website.

Date:_____(YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the *Employment Equity Act*.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1. The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with HRSDC-Labour.

OR

( ) A5.2. The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to HRSDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to HRSDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for

Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions)

FORM 1 – BID SUBMISSION FORM
Conferencing & Operator Assisted Services (COAS) – RFP # xx

BID SUBMISSION FORM		
Bidder's full legal name ***Note to Bidders: Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder.]***		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Email	
Bidder's Procurement Business Number (PBN) ***[see the Standard Instructions 2003]*** ***[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]***	Clearance Level	
Security Clearance Level of Bidder ***[include both the level and the date it was granted]*** ***[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]***	Date Granted	
	Issuing Entity (PWGSC, RCMP, etc.)	
	Legal name of entity to which clearance issued	
Number of FTEs ***[Bidders are requested to indicate, the total number of full-time-equivalent positions that would be created and maintained by the bidder if it were awarded the Contract. This information is for information purposes only and will not be evaluated.]***		

Cloud Service Provider (CSP) ITS Assessment checklist:

1. Has the Bidder's proposed CSP completed an ISO 27001 **OR** SOC 2 Type II report (from the trust principles of security, availability, processing, and confidentiality) for the services required to deliver COAS?
   Yes ☐ No ☐
2. Has the Bidder's CSP completed an ITSM.50.062 Cloud Security Risk Management (at a minimum of Tier 1 / PA LL) for the services required to deliver COAS
   Yes ☐ No ☐

On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:

1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation;
2. This bid is valid for the period requested in the bid solicitation;
3. All the information provided in the bid is complete, true and accurate;
4. All the prices bid, on an individual basis, represent fair market value;
5. The information provided by the Bidder in its response to the Qualifying Criteria is true and accurate;
6. The Bidder agrees to submit within 5 FGWDs of a request by Canada, the following for CSP ITS Assessment:
   1. A complete ISO 27001 **OR** SOC 2 Type II report from the trust principles of security, availability, processing, and confidentiality.
   2. A complete ITSM.50.062 Cloud Security Risk Management at a minimum of Tier 1 (PA LL) for the services required to deliver COAS.
7. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.

Signature of Authorized Representative of Bidder	

If you are submitting a bid as a Joint Venture, please provide the information for each member on s separate Bid Submission Form

INTEGRITY FORM

Standard Instructions for Procurement Documents

Version 1.4

Date April 1, 2019

Shared Services Canada
Services partagés Canada

Canada

SHARED SERVICES CANADA

Standard Instructions for Procurement Documents No. 1.4

TABLE OF CONTENTS

SHARED SERVICES CANADA

Standard Instructions for Solicitations

When these Standard Instructions are incorporated by reference into any Shared Services Canada (SSC) solicitation, they form part of that solicitation as though they were expressly set out in it in full. Bidders should review the entire solicitation, including these Standard Instructions, carefully in order to ensure they submit compliant bids.

1. Standard Instructions for All Procurement Documents

1.1 Questions and Communications

a) **Single Point of Contact**: To ensure the integrity of the competitive procurement process, questions and other communications regarding the solicitation must be directed only to the Contracting Authority identified in the solicitation. Failure to comply with this requirement may result in the bid being declared non-compliant.

b) **Deadline for Asking Questions**: Unless otherwise indicated in the solicitation, all questions and comments regarding the solicitation must be submitted by email to the Contracting Authority no later than 10 Federal Government Working Days (FGWDs, defined below) before the closing date. Questions received after that time may not be answered.

c) **Content of Questions**: Bidders should reference as accurately as possible the numbered item of the solicitation to which the question relates. Bidders should explain each question in sufficient detail in order to allow Canada to provide an accurate answer. Any questions that a bidder believes include proprietary information must be clearly marked “proprietary” at each relevant item. Items identified as proprietary will be treated as such unless Canada determines that the question is not of a proprietary nature. Canada may edit the questions or may request that the bidder do so, so that the proprietary nature of the question is eliminated, and the edited question and answer can be provided to all bidders. Questions not submitted in a form that can be provided to all bidders may not be answered by Canada.

d) **Improvements to the Specifications**: If bidders believe that the specifications contained in the solicitation could be improved technically or technologically (or could result in greater savings if certain changes were made), bidders are invited to make suggestions, in writing, to the Contracting Authority. Bidders should clearly outline the suggested improvement as well as the reasons for the suggestion. Canada will have the right to accept or reject any or all suggestions and will make any changes through an amendment to the solicitation.

e) **Publication of Answers**: To ensure the consistency and quality of information provided to bidders, significant questions and the answers will be posted on the Government Electronic Tendering Service (GETS) as an amendment to the solicitation. In the alternative, if the solicitation was originally circulated directly to suppliers, these answers will be provided to the same suppliers directly by email.

1.2 Solicitation Documents

a) **Publication**:

i) SSC will normally make its procurement documents available for download through the Government Electronic Tendering Service (GETS). However, if SSC has established a suppliers’ list (e.g., by pre-qualifying certain suppliers), SSC may make

the procurement documents available directly to those pre-qualified suppliers, rather than making them available through the GETS. Also, for certain requirements subject to the National Security Exception, documents may not be published on the GETS in order to preserve the confidentiality of the requirement.

ii) SSC is not responsible for and will not assume any liabilities whatsoever for the information found on websites of third parties. If a Notice of Proposed Procurement, solicitation or related documentation published on the GETS is amended, SSC will not be sending notifications to bidders. Instead, SSC will post all amendments, including significant questions received and the answers on the GETS. Bidders are solely responsible for consulting the GETS regularly for the most up-to-date information. SSC will not be liable for any oversight by the bidder, nor for notification services offered by a third party. In the alternative, if the solicitation was originally circulated directly to suppliers by email, any amendments will be provided to the same suppliers directly by email.

b) **Entire Requirement**: The solicitation documents contain all the requirements relating to the solicitation. Any other information or documentation provided to or obtained by a bidder from any source are not relevant. The term "Work" means all the activities, services, goods, equipment, matters and things required to be done, delivered or performed by the successful bidder under any resulting contract.

c) **Previous Requirements**: Bidders should not assume that specifications or practices from previous procurements or contracts will continue to apply, unless they are described in the solicitation. Bidders should also not assume that their existing capabilities meet the requirements of the solicitation simply because they have met previous requirements.

d) **Conflict between Documents**: If there is a conflict between these Standard Instructions and the main body of the solicitation, the main body of the solicitation will prevail.

e) **Meaning of Federal Government Working Day (FGWD)**: A FGWD is a calendar day, except for Saturday, Sunday and the following holidays:

i) New Year's Day[1];

ii) Good Friday and Easter Monday;

iii) Victoria Day;

iv) St-Jean Baptiste Day[1];

v) Canada Day[1];

vi) 1st Monday in August;

vii) Labour Day;

viii) Thanksgiving Day;

ix) Remembrance Day[1];

x) Christmas Day[1]; and

xi) Boxing Day[2].

Notes:

[1]If this holiday occurs on a Saturday or Sunday, then the following Monday will be a holiday.

[2]If this holiday occurs on a Saturday, then the following Monday will be a holiday. If this holiday occurs on a Sunday or Monday, then the following Tuesday will be a holiday.

1.3 Applicable Laws

This procurement process and any resulting contract will be interpreted and governed, and the relations between the parties determined, by the laws in force in one of the provinces or territories of Canada. Each bidder may indicate in its Bid Submission Form which of the provinces or territories it wishes to apply. If the bidder does not indicate which province or territory it wishes to apply, the laws of the Province of Ontario will apply automatically.

1.4 The Bidder

a) **Definition of Bidder**: In the solicitation, "bidder" means the person or entity (or, in the case of a joint venture, the persons or entities) submitting a bid. It does not include the parent, subsidiaries or other affiliates of the bidder, or its subcontractors.

b) **Legal Capacity**: The bidder must have the legal capacity to contract. If the bidder is a sole proprietorship, a partnership or a corporate body, the bidder must provide, if requested by the Contracting Authority, any requested supporting documentation indicating the laws under which it is registered or incorporated, together with the registered or corporate name of the bidder and its place of business. This also applies to each entity submitting a bid as a joint venture.

c) **Joint Venture Bidders**: A joint venture is an association of two or more parties who combine their money, property, knowledge, expertise or other resources in a single joint business enterprise to submit a bid together. A bidder that is a joint venture must indicate clearly that it is a joint venture and provide the following information:

   i) the name of each member of the joint venture;

   ii) the Procurement Business Number of each member of the joint venture;

   iii) the name of the representative member of the joint venture (i.e., the member chosen by the other members to act on their behalf, if applicable); and

   iv) the name of the joint venture, if applicable.

   If this information is not clearly provided in the bid, the bidder must provide the information on request by the Contracting Authority. Canada may require that the bid and any resulting contract be signed by all the members of the joint venture unless one member has been appointed to act on behalf of all members of the joint venture. The Contracting Authority may, at any time, require that each member of the joint venture confirm that the representative member has been appointed with full authority to act as its representative for the purposes of the solicitation and any resulting contract. If a contract is awarded to a joint venture, all members of the joint venture will be jointly and severally or solidarily liable for the performance of any resulting contract.

d) **Bids not Assignable or Transferable**: Substitute bidders will not be accepted. The bidder will not be permitted to assign or transfer its bid.

e) **Procurement Business Number**: Bidders are required to have a Procurement Business Number (PBN) before the award of any resulting instrument (whether it is a contract, standing offer, etc.). Suppliers may register for a PBN online at Supplier Registration Information. For non-Internet registration, suppliers may contact the InfoLine at 1-800-811-1148 to obtain the telephone number of the nearest Supplier Registration Agent.

f) **Submission of Ownership and Control Information**: If the solicitation concerns a procurement that is subject to the National Security Exception under Canada's trade agreements, the bidder must provide, if requested by the Contracting Authority, the following information as well as any other requested information related to the ownership and control of the bidder, its owners, its management and any "related" (see definition below) corporations and partnerships:

i) an organization chart for the bidder showing all related corporations and partnerships;

ii) a list of all the bidder's shareholders and/or partners, as applicable; if the bidder is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner(s); and

iii) a list of all the bidder's directors and officers, together with each individual's home address, date of birth, birthplace and citizenship(s); if the bidder is a subsidiary, this information must be provided for each parent corporation or partnership, up to the ultimate owner(s).

In the case of a joint venture bidder, this information must be provided for each member of the joint venture. The Contracting Authority may also require that this information be provided in respect of any subcontractors specified in a bid. For the purposes of this section, a corporation or partnership will be considered related to another party if:

(A) they are "related persons" or "affiliated persons" according to the Canada *Income Tax Act*;

(B) the entities have now or in the two years before the closing date had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

(C) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

1.5 Bid Costs

Canada will not reimburse any bidder for costs incurred to prepare or submit a bid. These costs, as well as any costs incurred by bidders in relation to the evaluation of the bid, are the sole responsibility of bidders. Any expenses that the bidder incurs in relation to any resulting contract or other instrument prior to the award of that instrument are entirely at the risk of the bidder.

1.6 Conference for Interested Suppliers

If the solicitation states that a conference for interested suppliers will be held, the following applies:

a) The solicitation will indicate the place, date and time for the conference.

b) At the conference, aspects of the requirement outlined in the solicitation will be reviewed and suppliers will be able to raise questions.

c) Bidders are requested to communicate with the Contracting Authority before the conference to indicate if they will attend the conference. Bidders should provide to the Contracting Authority, by email, the names of the representative(s) who will be attending and a list of issues they wish to discuss at least 3 FGWDs before the conference.

d) A maximum of 4 representatives from each bidder may attend the conference. The bidder's representatives may include one or more subcontractors.

e) Canada will issue an amendment to the solicitation if there are any clarifications or changes to the solicitation discussed at or resulting from the conference.

f) Canada recommends that all bidders participate in the conference, but bidders can submit a bid regardless of whether or not they attend the conference.

1.7 Site Visit

If the solicitation states that a site visit will be held, the following applies:

a) The solicitation will indicate the place, date and time for the site visit.

b) The solicitation will indicate whether the site visit is optional or mandatory. If the site visit is optional, bidders can submit a bid regardless of whether or not they attend the site visit. If the site visit is mandatory, only bidders that attend the site visit are eligible to submit a bid.

c) Bidders are requested to communicate with the Contracting Authority before the site visit to indicate if they will attend the site visit. Bidders should provide to the Contracting Authority, by email, the names of the representative(s) who will be attending at least 3 FGWDs before the site visit.

d) A maximum of 4 representatives from each bidder may attend the site visit. The bidder's representatives may include one or more subcontractors.

e) Bidders who do not confirm their intention to attend and provide the name(s) of the representative(s) who will attend as required will not be allowed access to the site.

f) Canada will issue an amendment to the solicitation if there are any clarifications or changes to the solicitation resulting from the site visit.

g) Bidders may be asked to sign an attendance form at the site visit.

1.8 Bids

a) **Submission in Sections**: Canada requests that each bidder submit its bid in the following separate sections, as applicable:

   i) Technical Bid;

   ii) Financial Bid; and

   iii) Certifications.

b) **Products Bid**: Unless otherwise specified in the solicitation, all products bid must be products in current production by the bidder or by the applicable manufacturer. Claims in a bid that a future upgrade or release of any of product included in the bid will meet the mandatory requirements of the solicitation, where the upgrade or release is not available on the closing date, will not be considered.

c) **Prices and Financial Bid**:

   i) Canada requests that the bidder include prices only in its financial bid.

   ii) Unless otherwise indicated in the solicitation, bidders must include a single, firm, all-inclusive price in each cell requiring an entry in the pricing tables.

   iii) Unless the solicitation specifically contemplates bids in foreign currency, all prices must be quoted in Canadian dollars. If the solicitation does not contemplate bids in

foreign currency, and the bid is unclear regarding the currency used, Canada will treat the quoted prices as being in Canadian dollars.

iv) Unless otherwise indicated in the solicitation, bidders' prices must exclude any applicable taxes and will be evaluated on that basis.

v) Unless otherwise indicated in the solicitation, prices must also be FOB destination, Canadian customs duties and excise taxes included.

vi) If the bidder wishes to provide an item at no cost, the bidder should insert $0.00 in the applicable pricing cell.

vii) Unless otherwise indicated in the solicitation, the bidder should prepare its financial bid on the basis that every line item with a price can be ordered separately.

viii) The financial bid must include all costs for the requirement described in the solicitation for the entire resulting contract period, including any option years. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the solicitation and the associated costs of these items is the sole responsibility of the bidder.

d) **Format for each Section**: Canada requests that bidders follow these format guidelines:

i) use 8.5 x 11 inch paper;

ii) use a numbering system that corresponds to the solicitation;

iii) include a title page at the front of each section of the bid that includes the title, date, solicitation number, bidder's name and address and contact information of its representative; and

iv) include a table of contents.

e) **Signature of Bid**: Canada requires that each bid be signed by the bidder or by an authorized representative of the bidder. If a bid is submitted by a joint venture, it must be signed in accordance with the Subsection above entitled "**Joint Venture Bidders**". If the bid is not signed at the time it is submitted, the bidder must sign the bid if requested by the Contracting Authority.

f) **Canada's Policy on Green Procurement**: In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. To assist Canada in reaching its objectives, Canada requests that bidders use paper containing fibre certified as originating from a sustainably-managed forest and/or containing a minimum of 30% recycled content.

g) **Bid Validity Period**: By submitting a bid, the bidder agrees that its bid will remain open for acceptance at least 60 calendar days from the closing date of the solicitation, unless otherwise specified in the solicitation. If the solicitation is an Invitation to Qualify, there is no validity period and Canada will assume that all respondents wish to qualify unless they withdraw in writing.

h) **Extensions to the Bid Validity Period**: Canada may seek an extension of the bid validity period from all compliant bidders in writing at least 48 hours before the end of the bid validity period. If the extension is accepted by all compliant bidders, Canada will continue with the evaluation of the bids. If the extension is not accepted by all compliant bidders, Canada will, at its sole discretion, either continue with the evaluation only of the bids that have been extended or cancel the solicitation.

i) **Language of Bid**: Bid documents and supporting information may be submitted in either English or French.

j) **Property of Canada**: Every bid received by SSC, whether received on time or not (and regardless of the format in which the bid is received), will become the property of Canada and will not be returned. A bidder may mark any portions of its bid that it considers to be confidential. All bids are subject to the provisions of the *Access to Information Act* and any other applicable laws.

k) **Bids Must Be Complete**: Unless otherwise specified in the solicitation, Canada will evaluate only the documentation provided with the bid. Canada will not consider information such as references to website addresses where additional information can be found, or technical manuals or brochures not submitted with the bid. Canada will not sign any confidentiality agreement or non-disclosure agreement submitted within a bid and will not evaluate any documentation that is subject to such agreements.

l) **Modification of Bids**: Bids can be modified, withdrawn or resubmitted, during the bidding period, up until the solicitation closing date and time. A bid withdrawn after the solicitation closing date and time cannot be resubmitted.

1.9 Security Clearance – General Requirements

a) **Security Clearance Requirements**: The bidder must meet the security clearance requirements described in the solicitation. The solicitation will indicate whether the bidder must meet these requirements on the closing date, or before a contract is awarded. If the solicitation does not indicate when the requirement must be met, the requirements must be met before a contract is awarded.

b) **Timing**: Bidders should take steps to obtain the required security clearance promptly. If the security clearance requirements are required before the award of a contract, then any delay in the award of a contract to allow the successful bidder to obtain the required clearance will be at the sole discretion of SSC.

c) **PSPC Conducts Clearance Process**: SSC has an arrangement with Public Services and Procurement Canada to process security clearances, and does not control the process itself. It can be a lengthy process and bidders should initiate it as soon as possible. For additional information on security requirements, Bidders should refer to the Industrial Security Program website at http://ssi-iss.tpsgc-PSPC.gc.ca/index-eng.html.

d) **Joint Venture Bidder**: Unless otherwise specified in the solicitation, in the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

1.10 Bidder Responsibilities

Each bidder is responsible for:

a) obtaining clarification of the requirements contained in the solicitation, if necessary, before submitting a bid;

b) preparing its bid in accordance with the instructions contained in the solicitation;

c) submitting a complete bid by the closing date and time;

d) properly addressing and submitting its bid;

e) ensuring that the bid clearly indicates the bidder's name, address, and contact information for the bidder's representative, as well as the solicitation number;

f) providing a comprehensible and sufficiently detailed bid, including all requested pricing details, that will permit a complete evaluation in accordance with the criteria set out in the solicitation.

1.11 General Rights of Canada

In addition to any other rights described in the solicitation, Canada has the right to:

a) reject any or all bids received in response to the solicitation;

b) negotiate with bidders on any or all aspects of their bids;

c) conduct an electronic auction;

d) accept any bid in whole or in part without negotiations;

e) cancel the solicitation at any time;

f) reissue the solicitation;

g) if no compliant bids are received and the requirement is not substantially modified, reissue the solicitation by inviting only those suppliers who submitted bids in response to the solicitation to submit new bids within a period designated by Canada; and

h) negotiate with the sole compliant bidder to ensure best value to Canada.

1.12 Conduct of the Evaluation

a) **Assessment of Bids**:

i) Bids will be assessed in accordance with all the requirements described in the solicitation, including the evaluation criteria.

ii) If the bid solicitation describes several steps in the evaluation process, Canada may conduct steps of the evaluation in parallel. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the bidder has successfully passed all the previous steps.

iii) Each bid will be reviewed to determine whether it meets the mandatory requirements of the solicitation. Any element of the solicitation identified with the words "**must**" or "**mandatory**" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-compliant and be disqualified. Once a bid has been declared non-compliant, Canada will have no obligation to evaluate the bid further.

iv) If the solicitation includes rated requirements, then each bid will be rated by assigning scores to the rated requirements, which are identified in the solicitation by the word "**rated**" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by the solicitation will be rated accordingly.

b) **Evaluation Team**: An evaluation team composed of representatives of Canada will evaluate the bids. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

c) **Discretionary Rights during Evaluation**: In conducting its evaluation of the bids, Canada may, but will have no obligation to, do the following:

i) request additional information substantiating the compliance of the bid with any mandatory requirement, if that substantiation was not required to be included in the bid submitted on the closing date;

ii) seek clarification or verification from bidders regarding any or all information provided by them with respect to the solicitation;

iii) contact any or all references supplied by bidders to verify and validate any information submitted by either bidders or their references (if contact information for references is not required to be included in the bid submitted on the closing date, the bidder must provide that information during evaluation upon request by the Contracting Authority);

iv) request, before award of any contract, specific information with respect to any bidder's legal status;

v) conduct a survey of any bidder's facilities and/or examine their technical, managerial, and financial capabilities to determine if they are adequate to meet the requirements of the solicitation and adequate to perform the Work (as described in any resulting contract clauses included in the solicitation);

vi) correct any error in the extended pricing of bids by using unit pricing and correct any error in quantities in bids to reflect the quantities stated in the solicitation; in the case of an error in the extension of prices, the unit price will be used;

vii) if the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by any bidder into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by that bidder;

viii) treat any blank pricing cell in any pricing tables provided by bidders as $0.00. Canada may request that the bidder confirm that the price is, in fact, $0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is $0.00 will be declared non-compliant;

ix) verify any information provided by bidders through independent research, use of any government resources, or by contacting third parties;

x) verify with the supplier that it satisfies the conditions for participation and is capable of fulfilling the terms of the contract at the price bid If Canada receives a bid from a supplier with a price that is abnormally lower than the prices in other bids;.and

xi) interview, at the sole cost of the bidder, any bidder and/or any or all of the resources proposed by the bidder to fulfill any requirement of the solicitation, for the purpose of determining whether the resource meets the requirements set out in the solicitation (if contact information for individual resources is not required to be included in the bid submitted on the closing date, the bidder must provide that information during evaluation upon request by the Contracting Authority).

d) **Time to Respond**: Bidders will have the number of FGWDs specified in the request by the Contracting Authority to comply with any request for clarification, verification or additional information. Unless the bid solicitation specifies another time for responding, the following time periods apply:

i) **Requests for Clarifications**: If Canada seeks clarification or verification or additional information from the bidder about its bid, the bidder will have 2 FGWDs (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Depending on the nature of the request, failure to meet this deadline may result in the bid being declared non-compliant.

ii) **Requests for Survey**: If Canada wishes to survey the bidder's facilities, the bidder must make its facilities available for this purpose within 5 FGWDs of a request by the Contracting Authority.

e) **Extension of Time to Respond**: If additional time is requested by a bidder, the Contracting Authority may grant an extension in his or her sole discretion.

f) **Evaluation of Joint Venture Experience**:

i) If the bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and M. A solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and M), the bidder has previously done this work. This bidder can use this experience to meet the requirement (even if neither L nor M has met this experience requirement on its own). If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

ii) A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this solicitation. Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself.

Example A: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service, and (b) that the bidder have 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-compliant.

Example B: A bidder is a joint venture consisting of members A and B. If a solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting one of the following:

(A) Contracts all signed by A;

(B) Contracts all signed by B; or

(C) Contracts all signed by A and B in joint venture;

(D) Contracts signed by A and contracts signed by A and B in joint venture; or

(E) Contracts signed by B and contracts signed by A and B in joint venture,

that collectively show a minimum of 100 billable days of providing resources.

iii) Wherever substantiation of a criterion is required, the bidder is requested to indicate which joint venture member satisfies the requirement. If the bidder has not identified which joint venture member satisfies any given requirement, the Contracting Authority will provide an opportunity to the bidder to submit this information during the

evaluation period. If the bidder does not submit this information within the period set by the Contracting Authority, its bid will be declared non-compliant.

iv) Any bidder with questions regarding the way in which a joint venture bid will be evaluated should submit their questions as early as possible during the solicitation period.

1.13 Canada's Right to Require a Demonstration

a) Canada may, but will have no obligation to, require that the top-ranked bidder (identified after the financial evaluation) demonstrate any of the features, functionalities or capabilities described in the solicitation or in its bid, in order to permit Canada to verify its compliance with the requirements of the solicitation.

b) If required by Canada, the demonstration must be conducted, at no cost to Canada, at a location in Canada agreed to by the Contracting Authority.

c) Canada will provide at least 5 FGWDs of notice before the scheduled date for the demonstration. The demonstration must be conducted during normal business hours, to be determined by the Contracting Authority. Once the demonstration has begun, it must be completed within 2 FGWDs.

d) Canada will pay its own travel and salary costs associated with any demonstration.

e) Despite the written bid, if Canada determines during a demonstration that any aspect of the top-ranked bidder's proposed solution does not meet the mandatory requirements of the solicitation, the bid will be declared non-compliant. If there are rated requirements in the solicitation, the following applies:

i) Canada may, as a result of a demonstration, reduce the top-ranked bidder's score on any rated requirement, if the demonstration indicates that the score provided to the top-ranked bidder on the basis of its written bid is not validated by the demonstration;

ii) The top-ranked bidder's score will not be increased as a result of any demonstration; and

iii) If the top-ranked bidder's score is reduced by the demonstration, Canada will reassess the ranking of all bidders.

If the top-ranked bidder is disqualified or is no longer the top-ranked bidder for any reason, the next-ranked compliant bidder will become the top-ranked bidder and will be subject to this Section.

1.14 Canada's Right to Require the Submission of a Sample

a) Canada may, but will have no obligation to, require that the top-ranked bidder (identified after the financial evaluation) provide a sample of the goods that it has bid (or goods that will form part of its solution), to allow Canada to verify compliance of the product or solution with any of the requirements of the solicitation or described in the bid by testing or examining the sample.

b) If required by Canada, the sample must be delivered, at no cost to Canada, to a location in Canada specified by the Contracting Authority, within 5 FGWDs of the Contracting Authority's request. The bidder must provide the Contracting Authority with all passwords or other information required in order to test and examine the sample. Canada may request that the bidder attend at the testing or examination of the sample.

c) Despite the written bid, if Canada determines as a result of testing or examining the sample that the top-ranked bidder's proposed product or solution does not meet the mandatory requirements of the solicitation, the bid will be declared non-compliant. If there are rated requirements in the solicitation, the following applies:

   i) Canada may, as a result of examining the sample, reduce the top-ranked bidder's score on any rated requirement, if the examination of the sample indicates that the score provided to the top-ranked bidder on the basis of its written bid is not validated by the examination;

   ii) The top-ranked bidder's score will not be increased as a result of the examination of any sample; and

   iii) If the top-ranked bidder's score is reduced by the examination of the sample, Canada will reassess the ranking of all bidders.

   If the top-ranked bidder is disqualified or is no longer the top-ranked bidder for any reason, the next-ranked compliant bidder will become the top-ranked bidder and will be subject to this Section.

d) Unless otherwise indicated, Canada will return the sample to the bidder (or make the sample available for pick-up) after the solicitation process is completed. If requested, and the examination or testing of the sample involved deploying the sample in circumstances in which Canada's data was stored on the sample, the bidder must work with Canada to remove any of Canada's data from the sample.

1.15 Requirements related to Previous Corporate Experience of the Bidder

If the solicitation requires that the bid demonstrate previous experience of the bidder, the following applies unless otherwise specified in the solicitation. The previous experience will only be awarded points or considered to demonstrate the required experience in the following circumstances:

a) the experience must have been obtained by (i.e., the relevant work must have been completed by) the bidder itself. Work performed by any proposed subcontractor or any affiliate of the bidder or any corporate predecessor will not be evaluated, unless (with respect to a corporate predecessor) the bidder can demonstrate that:

   i) the corporate predecessor amalgamated with one or more other corporations to form the bidder or another corporate predecessor that meets the requirements set out in this Subsection (a); or

   ii) the bidder acquired all or substantially all of the assets and personnel of the corporate predecessor that were involved in completing the work related to the experience.

   Canada may request additional information about corporate predecessors during evaluation.

b) the work was completed by the closing date;

c) the bid includes, as a minimum, the name of an individual from the customer reference who will act as a reference; and

d) if more examples of previous experience (e.g., multiple projects) are provided in the bid than were requested by the solicitation, Canada will ask the bidder which one(s) to evaluate. If the bidder does not respond within the time allocated by the Contracting Authority, Canada will decide in its discretion which one(s) will be evaluated.

1.16 Requirements relating to Résumés

If the solicitation requires the submission of résumés for individual resources, the following applies unless otherwise specified in the solicitation:

a) Proposed resources must be employees of the bidder or employees of a subcontractor. In the alternative, proposed resources may be independent contractors to whom the bidder would subcontract a portion of the Work, but in this case they must have confirmed to the bidder that they are willing to participate in the bid and to perform the work if a contract is awarded. Canada may require further information in this regard during the evaluation, including confirmation from individual resources regarding their status.

b) For educational requirements for a particular degree, designation or certificate, Canada will only consider educational programmes that were successfully completed by the resource by the closing date. If the degree, designation or certification was issued by an educational institution outside of Canada, the bidder must provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC).

c) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the closing date and must continue, where applicable, to be a member in good standing of the profession or membership throughout the evaluation period and resulting contract period. Where the designation or membership must be demonstrated through a certification, diploma or degree, the document must be current, valid and issued by the entity specified in the solicitation. If the entity is not specified, the issuer must have been an accredited or otherwise recognized body, institution or entity at the time the document was issued. If the degree, diploma or certification was issued by an educational institution outside of Canada, the bidder must provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC).

d) For work experience, Canada will not consider experience gained as part of an educational programme, except for experience gained through a formal co-operative programme at a post-secondary institution.

e) For any requirements that specify a particular time period (e.g., 2 years) of work experience, SSC will disregard any information about experience if the bid does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource participated.

f) For work experience to be considered by Canada, the bid must not simply indicate the title of the individual’s position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. In situations in which a proposed resource worked at the same time on more than one project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

1.17 Evaluation Procedures for Customer Reference Checks

a) Unless otherwise provided in the solicitation, Canada may choose, in its discretion, to conduct one or more customer reference checks.

b) Canada will conduct reference checks in writing by email (unless the contact person for the reference is only available by telephone). Canada will send all email reference check requests to contacts supplied by the bidders on the same day using the email address(es) provided in the bid (in the case of any telephone reference checks, Canada will contact the reference as soon as possible after email reference checks have been sent, but it may not occur on the same day).

c) If the information that Canada seeks to confirm with a reference is mandatory, then Canada will declare the bid non-compliant if the response from the contact person at the reference is not received within 5 FGWDs of the date that Canada's email was sent (or within 5 FGWDs of leaving a voicemail message for a telephone reference).

d) If the information that Canada seeks to confirm with a reference relates to a rated requirement, then Canada will not award any points if the response from the contact person at the reference is not received within 5 FGWDs of the date that Canada's email was sent (or within 5 FGWDs of leaving a voicemail message for a telephone reference).

e) On the third FGWD after sending out the reference check request, if Canada has not received a response, Canada will notify the bidder by email, to allow the bidder to contact its reference directly to ensure that it responds to Canada within 5 FGWDs. If the individual named by a bidder is unavailable when required during the evaluation period, the bidder may provide the name and email address of an alternate contact person from the same customer. Bidders will only be provided with this opportunity once for each customer, and only if the originally named individual is unavailable to respond (i.e., the bidder will not be provided with an opportunity to submit the name of an alternate contact person if the original contact person indicates that he or she is unwilling or unable to respond). The 5 FGWDs will not be extended to provide additional time for the new contact to respond.

f) Wherever information provided by a reference differs from the information supplied by the bidder, the information supplied by the reference will be the information evaluated.

g) Points will not be allocated and/or a bidder will not meet any mandatory experience requirement (as applicable) if:

   i) the customer reference states he or she is unable or unwilling to provide the information requested; or

   ii) the customer reference is not a customer of the bidder itself (for example, the customer cannot be the customer of an affiliate of the bidder or a subcontractor to the bidder instead of being a customer of the bidder itself), unless the solicitation provides otherwise.

   Nor will points be allocated or a mandatory requirement be met if the customer is itself an affiliate or other entity that does not deal at arm's length with the bidder.

1.18 Evaluation Procedures for Proposed Equivalent Products

a) If the solicitation states that bidders must propose equipment that is specified by brand name, model and/or part number in order to ensure compatibility, interoperability and/or interchangeability with existing equipment owned by Canada, this Section applies regarding the evaluation of those products.

b) Products that are equivalent in form, fit, function and quality that are fully compatible, interchangeable, and interoperable with the existing equipment owned by Canada will be considered if the bidder:

i) clearly designates in its bid the brand name, model and/or part number of the proposed equivalent product;

ii) demonstrates in the written bid that the proposed equivalent is fully compatible, interoperates with, and is interchangeable with the item(s) specified in the solicitation;

iii) provides complete specifications and descriptive technical documentation for each equivalent item proposed;

iv) substantiates the compliance of its proposed equivalent by demonstrating that it meets all mandatory performance criteria that are specified in the solicitation; and

v) clearly identifies those areas in the specifications and descriptive technical documentation that demonstrate the equivalence of the proposed equivalent product.

c) If requested during evaluation, the bidder must submit a sample of any proposed equivalent product to the Contracting Authority for testing.

d) If requested during evaluation, the bidder must provide a demonstration of its proposed equivalent product.

e) Proposed equivalent products will be declared non-compliant if:

i) the bid fails to provide all the information required to allow the Contracting Authority to evaluate the equivalency of the proposed equivalent, including additional information requested by the Contracting Authority during the evaluation to supplement the information submitted in the bid (Note: it is the responsibility of the bidder to include all information required to evaluate equivalency as described above; however, all bidders acknowledge that Canada will have the right, but not the obligation, to request any additional information during the evaluation that it requires to make a determination regarding equivalency);

ii) the Contracting Authority determines that the proposed equivalent fails to meet or exceed the mandatory requirements specified in the solicitation; or

iii) the Contracting Authority determines that the proposed equivalent is not equivalent in form, fit, function or quality to the item(s) specified in the solicitation or that the proposed equivalent is not fully compatible, interoperable and interchangeable with any existing equipment owned by Canada that is specified in the solicitation.

1.19 Substitution of a Proposed Resource during Evaluation

a) If the bidder is unable to provide the services of an individual named in its bid due to the death, sickness, extended leave (including parental leave or disability leave), retirement, resignation or dismissal for cause of that individual, the bidder may propose a substitute to the Contracting Authority, by providing:

i) the reason for the substitution with substantiating documentation acceptable to the Contracting Authority;

ii) the name, qualifications and experience of a proposed replacement; and

iii) proof that the proposed replacement has the required security clearance granted by Canada, if applicable.

b) No more than one substitute will be considered for any given resource proposed in the bid prior to contract award. In response to the bidder's proposed substitution, the Contracting Authority may decide in its sole discretion either to:

i) set aside the bid and give it no further consideration; or

ii) evaluate the replacement in accordance with the requirements of the solicitation in the place of the original resource as if that replacement had originally been proposed in the bid, with any necessary adjustments being made to the evaluation results, including the rank of the bid vis-à-vis other bids.

c) If no substitute is proposed, or the proposed substitute does not meet the requirements of the solicitation, the Contracting Authority will disqualify the bid.

1.20 Rejection of a Bid not Offering Good Value and Price Justification

a) Canada may reject any bid if, in Canada's opinion, the bid does not offer good value to Canada.

b) If Canada receives only one compliant bid, the bidder must provide one or more (as requested) of the following forms of price justification, if requested by the Contracting Authority:

i) a current published price list indicating the percentage discount available to Canada;

ii) a copy of paid invoices for the same or similar quality and quantity of the goods, services or both sold to other customers;

iii) a price breakdown showing the cost of direct labour, direct materials, purchased items, engineering and plant overheads, general and administrative overhead, transportation, etc., and profit;

iv) price or rate certifications; or

v) any other supporting documentation requested by the Contracting Authority.

The bidder should provide this information within a reasonable period of time, not to exceed 10 FGWDs, unless the Contracting Authority has granted an extension.

1.21 Rejection for Failure to Pass Financial Capability Assessment

a) Canada may reject any bid if, in Canada's opinion, the bidder does not have the financial capability to perform the Work described in the resulting contract clauses of the solicitation.

b) To determine the bidder's financial capability, the Contracting Authority may, by written notice to the bidder, require the submission of some or all of the financial information detailed below during the evaluation of bids. The bidder must provide the following information to the Contracting Authority within 15 FGWDs of the request or any longer period specified by the Contracting Authority in the notice:

i) Audited financial statements, if available, or the unaudited financial statements (prepared by the bidder's outside accounting firm, if available, or prepared in-house if no external statements have been prepared) for the bidder's last three fiscal years, or for the years that the bidder 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.

ii) If the date of the financial statements in Subsection (i) above is more than five months before the date of the request for information by the Contracting Authority, the bidder must also provide, unless this is prohibited by legislation for public companies (in the relevant jurisdiction where the bidder was legally formed), the last quarterly financial statements (consisting of a Balance Sheet and a year-to-date Income Statement), as of two months before the date on which the Contracting Authority requests this information.

iii) If the bidder has not been in business for at least one full fiscal year, the following must be provided:

(A) the opening Balance Sheet on commencement of business (in the case of a corporation, the date of incorporation); and

(B) the last quarterly financial statements (consisting of a Balance Sheet and a year-to-date Income Statement) as of two months before the date on which the Contracting Authority requests this information.

iv) A certification from the Chief Financial Officer or an authorized signing officer of the bidder that the financial information provided is complete and accurate.

v) A confirmation letter from all of the financial institution(s) that have provided short-term financing to the bidder outlining the total of lines of credit granted to the bidder and the amount of credit that remains available and not drawn upon as of one month prior to the date on which the Contracting Authority requests this information.

vi) A detailed monthly Cash Flow Statement covering all the bidder's activities (including the requirement subject to the solicitation) for the first two years of the requirement that is the subject of the solicitation, unless this is prohibited by legislation (in the relevant jurisdiction where the bidder was legally formed). This statement must detail the bidder's major sources and amounts of cash and the major items of cash expenditures on a monthly basis, for all the bidder's activities. All assumptions made should be explained as well as details of how cash shortfalls will be financed.

vii) A detailed monthly Project Cash Flow Statement covering the first two years of the requirement that is the subject of the solicitation, unless this is prohibited by legislation (in the relevant jurisdiction where the bidder was legally formed). This statement must detail the bidder's major sources and amounts of cash and the major items of cash expenditures, for the requirement, on a monthly basis. All assumptions made should be explained as well as details of how cash shortfalls will be financed.

c) **Joint Venture**: If the bidder is a joint venture, the financial information required by the Contracting Authority must be provided by each member of the joint venture and each member must itself be financially capable.

d) **Subsidiary**: If the bidder is a subsidiary of another company, then any financial information required by the Contracting Authority by Subsection (b) must also be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the bidder. However, if the bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the bidder's financial capability because its financial information has been combined with its parent's, Canada may, in its sole discretion, award the contract to the bidder on the condition that one or more parent companies grant a performance guarantee to Canada.

e) **Financial Information Already on File at the Public Services and Procurement Canada**: SSC sometimes retains either Public Services and Procurement Canada (PSPC) or a third party to conduct financial capability assessments for SSC solicitations. In situations in which SSC confirms that PSPC is conducting the financial capability assessment, then the bidder is not required to resubmit any financial information requested by the Contracting Authority that is already on file at PSPC with the Contract Cost Analysis, Audit and Policy Directorate of the Policy, Risk, Integrity and Strategic Management Sector, provided that within the above-noted time frame:

i) the bidder identifies to the Contracting Authority in writing the specific information that is on file and the requirement for which this information was provided; and

ii) the bidder authorizes the use of the information for this requirement.

It is the bidder's responsibility to confirm with the Contracting Authority that this information is on file with PSPC. By doing so, the bidder consents to the PSPC sharing this information with SSC.

f) **Other Information**: Canada may request from the bidder any other information that Canada may require to conduct a complete financial capability assessment of the bidder.

g) **Confidentiality**: If the bidder provides the information required above to Canada in confidence while indicating that the disclosed information is confidential, then Canada will treat the information in a confidential manner to the extent permitted by the *Access to Information Act*, Subsections 20(1)(b) and (c).

h) **Security**: In determining the bidder's financial capability to fulfill this requirement, Canada may consider any security the bidder is capable of providing, at the bidder's sole expense (for example, an irrevocable letter of credit from a registered financial institution drawn in favour of Canada, a performance guarantee from a third party, or some other form of security, as determined by Canada).

1.22 Rejection of a Bid due to Conflict of Interest or Unfair Advantage

a) **Conflict of Interest or Unfair Advantage**: In order to protect the integrity of the procurement process, Canada may reject a bid if:

i) the bidder, any of its subcontractors, or any of their respective employees or former employees was involved in any manner in the preparation of the solicitation or in any situation of conflict of interest or appearance of conflict of interest; or

ii) the bidder, any of its subcontractors, or any of their respective employees or former employees had access to information related to the solicitation that was not available to other bidders and that would, in Canada's opinion, give or appear to give the bidder an unfair advantage.

Bidders who are in doubt about a particular situation should contact the Contracting Authority during the question period for the solicitation. By submitting a bid, the bidder represents that it does not consider itself to be in conflict of interest nor to have an unfair advantage. The bidder acknowledges that it is within Canada's sole discretion to determine whether a conflict of interest, unfair advantage or an appearance of conflict of interest or unfair advantage exists.

b) **Previous Experience**: The experience acquired by a bidder who is providing or has provided the same or similar goods and services described in the solicitation to Canada in the past will not, in itself, be considered by Canada as conferring an unfair advantage or creating a conflict of interest.

c) **Making Representations**: If Canada intends to reject a bid under this section, the Contracting Authority will inform the bidder and provide the bidder an opportunity to make representations before Canada makes a final decision. The Contracting Authority will provide the bidder with a minimum of 5 FGWDs to make its representations, which will normally be required in writing.

1.23 Rejection of a Bid due to National Interest or Security Considerations

If the solicitation concerns a procurement that is subject to the National Security Exception under Canada's trade agreements, Canada reserves the right to reject a bid if Canada is of the opinion that awarding the contract to the bidder could be injurious to the national interest or to national security.

1.24 Rejection of a Bid Prejudicing the Integrity and Fairness of the Process

a) SSC reserves the right to reject a bid if, in its opinion, there is sufficient evidence suggesting that the bidder has engaged in bid rigging or has otherwise colluded in the preparation of the bid. SSC's finding in this regard is not binding on the Competition Bureau or other departments. By participating in the solicitation process, the bidder agrees that SSC will not be liable for rejecting a bid on this basis, provided that SSC's decision was reasonable in light of the information considered at the time the decision was made.

b) SSC also reserves the right to reject a bid if, in its opinion, the inclusion of that bid in the evaluation has the effect of prejudicing the integrity and fairness of the procurement process (e.g., by distorting the evaluation or by causing an outcome that would not reasonably have been expected under prevailing market conditions or would not provide good value to Canada).

c) If Canada intends to reject a bid under this Section, the Contracting Authority will inform the bidder and provide the bidder an opportunity to make representations before making a final decision. The Contracting Authority will provide the bidder with a minimum of 5 FGWDs to make its representations, which will normally be required in writing.

1.25 Contract Award & Media Communications

a) All contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

b) The bidder agrees not to make any media announcements about the award of a contract without coordinating the announcement with the Contracting Authority.

1.26 Recourse for Bidders with respect to the Procurement Process

a) Suppliers are also encouraged to bring any concerns to the attention of the Contracting Authority.

b) Bidders with concerns with respect to the procurement process may also bring formal complaints to independent third parties. There is no single body that handles all types of procurement complaints, but rather several:

i) If the procurement is subject to the disciplines of any of Canada's domestic or international trade agreements and the bidder has standing under one or more of those trade agreements, the Canadian International Trade Tribunal reviews whether

or not Canada has violated any of its obligations under applicable trade agreements. More information can be found at http://www.citt-tcce.gc.ca/en/home.

ii) If the dollar value of the procurement is below the thresholds set by the *Canadian Free Trade Agreement*, but otherwise would have been covered by that trade agreement, a complaint may be made to the Office of the Procurement Ombudsman. More information can be found at: https://www.canada.ca/en/procurement-ombudsman.html.

iii) Recourse may also be available before the Federal Court of Canada or any of Canada's provincial superior courts.

c) Regardless of the forum to which a supplier brings a complaint, there are strict timelines for filing complaints. Additional information can be found at Canada's Buy and Sell website at www.buyandsell.gc.ca under the heading "Procurement Complaints".

2. Certifications

2.1 Deemed Certifications from Each Bidder

The following certifications are deemed to be provided by each bidder by virtue of submitting a bid, subject to any contrary indication in the solicitation. If a bid expressly indicates that the bidder is not providing these certifications, or the bid indicates that the certification is untrue, that bid will be declared non-compliant.

a) **Equipment and Software is "Off-the-Shelf"**: Any equipment and software bid to meet this requirement must be "off-the-shelf" (unless otherwise stated in the solicitation), meaning that each item of equipment and software is commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the equipment or software bid is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the closing date. By submitting a bid, the bidder is certifying that all the equipment and software bid is off-the-shelf.

b) **System is "Off-the-Shelf"**: Any system bid to meet this requirement must be "off-the-shelf" (unless otherwise stated in the solicitation), meaning that the equipment and software comprising any system bid must consist of standard equipment and software that are commercially available and require no further research or development. Together, this equipment and software must form part of an existing system with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the equipment or software comprising the system bid is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the closing date. By submitting a bid, the bidder is certifying that any system bid is off-the-shelf.

c) **Bidder's Proposed Resources will be Available**: By submitting a bid, the bidder certifies that, if it is awarded a contract as a result of the solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the solicitation or agreed to with Canada's representatives.

d) **Bidder has Verified Information about its Proposed Resources**: By submitting a bid, the bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the bidder to be true and accurate. Furthermore, the bidder warrants that every individual proposed by the bidder for the requirement is capable of performing the Work described in the resulting contract.

e) **Resources who are not Employees of the Bidder**: If a bidder has proposed any individual resource who is not an employee of the bidder, by submitting a bid, the bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the bidder and of the resource's availability. Failure to comply with the request may result in the bid being declared non-compliant.

2.2 Federal Contractors Program for Employment Equity

a) The Respondent must provide the Contracting Authority with a completed Federal Contractors Program for Employment Equity Certification before contract award. If the Respondent is a joint venture, the bidder must provide the Contracting Authority with this certification for each member of the joint venture. Bidders are requested to provide this certification in their Bid Submission Form.

b) By submitting a bid, the bidder certifies that the bidder (and each of the bidder's members, if the bidder is a joint venture), is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list (https://www.canada.ca/en/employment-social-development/programs/employment-equity/federal-contractor-program.html) available from Employment and Social Development Canada (ESDC). Canada will have the right to declare a bid non-compliant if the bidder (or any member of the bidder, if the bidder is a joint venture) appears on the "FCP Limited Eligibility to Bid" list at the time of contract award.

c) This information will not always be requested in an ITQ. For any ITQ, respondents should consult the ITQ and the Response Submission Form.

2.3 Former Public Servants

a) **TB Policy**: Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment receive special scrutiny, in order to ensure fairness in the spending of public funds. To comply with Treasury Board policies and directives on contracts with FPS, bidders must provide the information required below before contract award. Bidders are requested to provide this information in their Bid Submission Form.

b) **Definitions**: For the purposes of this Section,

"**former public servant**" is any former member of a department as defined in the *Financial Administration Act*, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

i) an individual;

ii) an individual who has incorporated;

iii) a partnership of former public servants; or

iv) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"**lump sum payment period**" means the period, measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the public service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"**pension**" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA) and any increases paid pursuant to the *Supplementary Retirement Benefits Act* as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, the *Defence Services Pension Continuation Act*, the *Royal Canadian Mounted Police Pension Continuation Act*, and the *Royal Canadian Mounted Police Superannuation Act*, the *Members of Parliament Retiring Allowances Act*, and that portion of pension payable to the *Canada Pension Plan Act*.

c) **Former Public Servant in Receipt of a Pension**: Based on the above definitions, the bidder is requested to indicate in its Bid Submission Form whether it is a FPS in receipt of a pension. If so, the bidder must provide the following information, for each FPS in receipt of a pension, as applicable:

i) name of former public servant;

ii) date of termination of employment or retirement from the Public service.

By providing this information, bidders agree that the successful bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with TB Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

d) **Work Force Adjustment Directive**: If the bidder is a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive, the bidder is requested to indicate this in its Submission Form. If so, the bidder must provide the following information:

i) name of former public servant;

ii) conditions of the lump sum payment incentive;

iii) date of termination of employment;

iv) amount of lump sum payment;

v) rate of pay on which lump sum payment is based;

vi) period of lump sum payment including start date, end date and number of weeks; and

vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

e) This information will not always be requested in an ITQ. For any ITQ, bidders should consult the ITQ and the Response Submission Form.

2.4 OEM Certification for Hardware

If indicated in the solicitation, the following certification is required to be provided:

a) If the bidder is the OEM for any item of hardware proposed as part of its bid, Canada requires that the bidder confirm in writing that it is the OEM for each item or group of items.

b) Any bidder that is not the Original Equipment Manufacturer (OEM) for every item of hardware proposed as part of its bid is required to submit the OEM's certification regarding the bidder's authority to provide and maintain the OEM's hardware, which must be signed by the OEM (not the bidder). No contract(s) resulting from any subsequent stage of this procurement process will be awarded to a bidder who is not the OEM of the hardware it proposes to supply to Canada, unless the OEM certification has been provided to Canada.

c) Bidders are requested to use the OEM Certification Form included with the solicitation to provide this certification. Although all the contents of the OEM Certification Form are required, using the form itself to provide this information is not mandatory. For bidders/OEMs who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the certification being declared non-compliant.

d) If the hardware proposed by the bidder originates with multiple OEMs, a separate OEM certification is required from each OEM.

e) Unless otherwise indicated in the solicitation, for the purposes of this procurement process, "**OEM**" means the manufacturer of the hardware, as evidenced by the name appearing on the hardware and on all accompanying documentation.

2.5 Software Publisher Certification and Software Publisher Authorization

If indicated in the solicitation, the following certification is required to be provided:

a) If the bidder is the Software Publisher for any of the proprietary software products identified in its bid, Canada requires that the bidder confirm in writing that it is the Software Publisher.

b) Any bidder that is not the Software Publisher of all the proprietary software products proposed as part of its bid is required to submit proof of the Software Publisher's authorization, which must be signed by the Software Publisher (not the bidder). No contract(s) will be awarded to a bidder that is not the Software Publisher of all of the proprietary software it proposes to supply to Canada, unless proof of this authorization has been provided to Canada. If the proprietary software proposed by the bidder originates with multiple Software Publishers, authorization is required from each Software Publisher.

c) Bidders are requested to use the Software Publisher Certification Form included with the solicitation to provide this certification. Although all the contents of the Software Publisher Certification Form are required, using the form itself to provide this information is not mandatory. For bidders who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided. Alterations to the statements in the form may result in the certification being declared non-compliant.

d) Unless otherwise indicated in the solicitation, for the purposes of this procurement process, "**Software Publisher**" means the owner of the copyright in any software products proposed in the bid, who has the right to license (and authorize others to license/sub-license) its software products.

2.6 Code of Conduct for Procurement

The Public Services and Procurement Canada *Code of Conduct for Procurement* (http://www.tpsgc-pwgsc.gc.ca/app-acq/cndt-cndct/index-eng.html) provides that bidders must respond to solicitations in an honest, fair and comprehensive manner, accurately reflect their capacity to satisfy the requirements set out in the solicitation and resulting contract, and submit bids and enter into contracts only if they will fulfill all obligations of the contract. A certification has been included in the Bid Submission Form in this regard. Failure of a bidder to comply with the *Code of Conduct for Procurement* may render its bid non-compliant.

2.7 Verification of Certifications

The certifications provided by bidders to Canada are subject to verification by Canada at all times. Canada will declare a bid non-compliant, and will be entitled to terminate any resulting contract for default, if any certification made by the bidder during the procurement process (whether made knowingly or unknowingly) is found to be untrue either during the bid evaluation period or during the resulting contract, standing offer, or supply arrangement period, as applicable. The Contracting Authority will have the right to ask for additional information to verify the bidder's certifications. Failure to comply with this request will render the bid non-compliant or will constitute a default under any resulting instrument that may be issued during a subsequent phase of the procurement process.

3. Standard Instructions for Invitations to Qualify

3.1 Terminology for Invitations to Qualify

a) the word "bidder(s)" in this document is replaced with the word "respondent(s)";

b) the word "bid(s)" in this document is replaced with the word "response(s)";

c) the "Invitation to Qualify" is simply a solicitation of interest, not a request for bids or tenders; and

d) there is no bid validity period, since an Invitation to Qualify invites respondents simply to qualify.

4. Standard Instructions for a Requests for Standing Offers (RFSO)

4.1 Nature of a Standing Offer

a) One method of supply used by Canada is to arrange with suppliers to submit an offer to provide goods, services or both during a specified period. Specific departments and agencies may then be authorized by SSC to make call-ups against the standing offer specifying the exact quantities of goods or level/type of services they wish to order at a particular time during the effective period of the standing offer in accordance with the predetermined terms and conditions set out in the standing offer.

b) A request for standing offers is an invitation to suppliers to make an offer to Canada.

c) A standing offer is not a contract for the acquisition or provision of any goods or services. Rather, it establishes a framework pursuant to which Canada can make one or more individual call-ups for the goods and services offered in the standing offer, each of which results in a separate contract.

d) The quantity of goods, level of services and estimated expenditure specified in the request for standing offers are only an approximation of potential future requirements given in good faith. The request for standing offers does not commit Canada to authorize the use of a standing offer by one or more departments or to issue one or more call-ups for any goods, services or both.

4.2 Terminology for Requests for Standing Offers

If the solicitation is a Request for Standing Offers, then:

a) the word "bidder(s)" in this document is replaced with the word "offeror(s)";

b) the word “bid(s)” in this document is replaced with the word “offer(s)”;

c) the term “Contracting Authority” in this document is replaced with the term “Standing Offer Authority”;

d) the offer validity period does not refer to the validity of any resulting standing offer if some are issued by Canada; rather, it refers to the period during which Canada may consider the proposed standing offer in order to determine whether or not to issue a resulting standing offer against which Canada may make call-ups.

5. Standard Instructions for Requests for Supply Arrangements (RFSAs)

5.1 Nature of a Supply Arrangement

a) A supply arrangement is a method of supply used by Canada to procure goods and services. A supply arrangement is an arrangement between Canada and pre-qualified suppliers that allows Canada to solicit bids from a pool of pre-qualified suppliers for specific requirements within the scope of a supply arrangement. A supply arrangement is not a contract for the provision of the goods and services described in it, but creates a source list for future solicitations.

b) Supply arrangements may include a set of pre-determined terms and conditions that will apply to subsequent solicitations and contracts. Each solicitation issued pursuant to a supply arrangement results in a separate contract. Supply arrangements may include ceiling prices, which may be lowered based on an actual requirement or the scope of work described in an individual solicitation.

5.2 Terminology for a Request for Supply Arrangement

If the solicitation is Request for Supply Arrangements, then:

a) the word “bidder(s)” in this document is replaced with the word “supplier(s)”;

b) the word “bid(s)” in this document is replaced with the word “response(s)”;

c) the term “Contracting Authority” in this document is replaced with the term “Supply Arrangement Authority”;

d) the response validity period does not refer to the validity of any resulting supply arrangement if some are issued by Canada; rather, it refers to the period during which Canada may consider the proposed supply arrangement in order to determine whether or not to issue a resulting supply arrangement that pre-qualifies the supplier for solicitations issued under the framework of the resulting supply arrangements; and

e) if the Supply Arrangement provides that SSC Clients may conduct solicitations under the supply arrangement directly, then with respect to individual bid solicitations issued pursuant to the Supply Arrangement by another department, all references to SSC in these Standard Instructions will be interpreted as references to the SSC Client conducting the solicitation.

6. Standard Instructions and Conditions for Telecommunications Procurements

6.1 Regulatory Framework

a) Canada recognizes that bidders may be subject to regulation by the Canadian Radio-television and Telecommunications Commission (CRTC) in respect of some or all of the services or products required under the solicitation. As a result, the bidder may:

i) be subject to regulation by the CRTC, but not require CRTC tariff approval to provide the services or products it proposes to Canada in its bid;

ii) be subject to regulation by the CRTC and propose services or products to Canada in its bid in accordance with an existing tariff that has already been approved by the CRTC; or

iii) be subject to regulation by the CRTC and propose services or products to Canada in its bid in accordance with a new tariff (or an amendment to an existing tariff) that has not yet been approved by the CRTC.

b) Despite the fact that individual bidders may be regulated differently by the CRTC, or that individual bidders' existing tariffs may be inconsistent with Canada's requirements, all bids will be evaluated in accordance with the evaluation process described in the solicitation.

6.2 Bidders' Responsibilities in Relation to Regulatory Framework

a) It is the sole responsibility of the bidder to:

i) identify any CRTC regulations or rulings to which it may be subject in relation to the solicitation and any resulting contract;

ii) obtain all approvals required to allow the bidder to deliver the services and products at the prices it proposes in its bid; and

iii) raise with Canada, during the question period for the solicitation, any concerns about conflicts between the solicitation (including the resulting contract clauses) and any CRTC regulations or rulings, by identifying:

(A) the specific requirement in the solicitation that creates the conflict; and

(B) the specific provisions of CRTC regulations or rulings that affect the solicitation requirement (including document titles, dates, page and paragraph numbers).

b) Bidders may wish, in preparing their bids, to seek interpretations from the CRTC if they are in doubt as to whether or not the services, products and prices they propose to Canada in their bid are subject to and in accordance with an existing tariff or require the filing of an amendment to an existing tariff or a new tariff.

c) The Contracting Authority will consider issues of conflicts between the requirements of the solicitation and CRTC regulations or rulings raised by bidders during the question period for the solicitation and may, in its sole discretion, amend the solicitation if it determines that amendments are consistent with Canada's operational requirements. However, Canada is not required to compromise its operational requirements to accommodate individual bidders' corporate or regulatory circumstances.

6.3 Regulatory Certifications for Bids including Non-regulated or Forborne Services or Products

Bidders proposing services, products and prices to Canada that are not subject to any tariff must provide the certification in Regulatory Form A.

6.4 Regulatory Certifications for Bids made under Existing Tariffs

a) Bidders proposing services, products and prices to Canada in accordance with an existing tariff that has already been approved by the CRTC must provide the following:

   i) a complete copy of the tariff or the specific URL where that tariff can be found, together with any information required to identify the tariff; and

   ii) the certification set out in Regulatory Form B.

b) Following the closing date, during the evaluation period, the bidder must immediately advise the Contracting Authority of any ruling from the CRTC relating to this tariff that affects its ability to provide the services, products or prices proposed in its bid.

6.5 Regulatory Certifications for Bids made under Tariffs not yet Approved by the CRTC

a) Bidders proposing services, products and prices to Canada in their bid under a proposed new tariff (or an existing tariff and a proposed amendment to that tariff) not yet approved by the CRTC must provide the following:

   i) a complete copy of the proposed new tariff (or the existing tariff and the proposed amendment to that existing tariff) or the specific URL where that tariff can be found, together with any information required to identify the tariff; and

   ii) the certification set out in Regulatory Form C.

b) The bidder is requested to include in its bid its best pre-estimate of the date by which the proposed new tariff or amendment will likely be approved by the CRTC. This pre-estimate is for information purposes only.

c) Following the closing date, during the evaluation period, the bidder must immediately advise the Contracting Authority of any ruling from the CRTC relating to this tariff that affects its ability to provide the services, products or prices proposed in its bid.

6.6 Evaluation Procedures for Bids based on a Draft Tariff

a) The following procedures apply to the top-ranked bid identified according to the evaluation process described in the solicitation, if some or all of the proposed services or products will be subject to a proposed new tariff or an existing tariff subject to a proposed amendment (collectively referred to as the "**Draft Tariff**").

b) Unless the bidder receives approval sooner, the Contracting Authority will allow no less than the following time period for the bidder to obtain interim approval of the Draft Tariff from the CRTC:

   i) if the CRTC considers the application on an ex parte basis, no fewer than 45 FGWDs following the closing date; or

   ii) if the CRTC uses a public process to consider the application, no fewer than 60 FGWDs following the closing date.

Following this period, the Contracting Authority may, at any time, require the bidder to obtain interim approval from the CRTC on 10 FGWDs' notice. The Contracting Authority may, in its sole discretion, extend this 10-FGWD period. In determining whether or not to grant such an extension, the Contracting Authority may request from the bidder any information it requires to consider the request and the impact of the request on Canada's operational requirements. The time periods described above (including extensions authorized by the Contracting Authority) are collectively referred to as the "**Allotted Approval Time**".

c) If the bidder does not, within the Allotted Approval Time, obtain interim approval of the Draft Tariff from the CRTC, the Contracting Authority will declare the bid non-compliant.

d) If, in the Allotted Approval Time, a bidder receives interim approval of its Draft Tariff in the form in which it was filed (i.e., the CRTC's interim approval is not subject to conditions and the bidder was not required to revise the Draft Tariff in order to obtain interim approval), the Contracting Authority will recommend the bid for contract award, subject to the provisions of the solicitation.

e) If, in the Allotted Approval Time, the bidder receives interim approval of its Draft Tariff, but the interim approval is subject to conditions or the bidder is required to revise the Draft Tariff in order to obtain interim approval, then:

i) the bidder must submit the following to the Contracting Authority (all within 5 FGWDs following the expiry of the Allotted Approval Time):

(A) the Draft Tariff in the form approved by the CRTC or the specific URL where that tariff can be found, together with any information required to identify the tariff;

(B) a list of any conditions subject to which the CRTC has given the interim approval;

(C) a list of all revisions made to the version of the Draft Tariff originally submitted with the bid and an explanation of how these changes affect the bid; and

(D) Regulatory Form D.

ii) Canada will review this submission and, in respect of the aspects of the bid that are affected by the revisions, Canada will determine whether the amendments to the original Draft Tariff affect:

(A) the bidder's compliance with the mandatory requirements of the solicitation;

(B) the bidder's score under the rated requirements of the solicitation, if any; or

(C) the bidder's ranking vis-à-vis other bidders in accordance with the evaluation process described in the solicitation.

iii) If Canada determines that the bidder remains compliant and that its ranking vis-à-vis other bidders has been unaffected by the amendments to the Draft Tariff, the Contracting Authority will recommend the bid for contract award, subject to the provisions of the solicitation.

iv) If Canada determines that, as a result of the revisions to the Draft Tariff, the bidder is either no longer compliant or is no longer the top-ranked bidder, Canada will proceed to consider the next-ranked bid for contract award, subject again to the provisions of the solicitation relating to the approval of any Draft Tariff.

v) If a contract is awarded on the basis of an interim approval of a Draft Tariff, Canada may request that all bidders that have submitted compliant bids extend the validity period of their bids until final approval is granted by the CRTC. If Canada terminates the contract as a result of the form of the CRTC's final approval of the Draft Tariff, Canada may, at its option:

(A) cancel the solicitation;

(B) award the contract to the next-highest-ranked bidder whose bid is still valid (i.e., a bid that the bidder extended or that was still valid without an extension), in accordance with the provisions of the solicitation; or

(C) reissue a solicitation for the requirement.

Bidders will have no obligation to extend the validity period for their bids. However, bidders who do not extend the validity period for their bids will not qualify for acceptance if Canada, following termination of the original contract, chooses option (B) above if their bid is no longer valid.

f) If, during the Allotted Approval Time, the CRTC provides final approval of the Draft Tariff, the same procedure will be followed that would apply if the CRTC had provided interim approval only.

g) This procedure has been developed in order to allow bidders who are required to submit new or revised tariffs to the CRTC to comply with the requirements of the solicitation to compete for this requirement. This procedure will also ensure that bidders have an opportunity, if the services or products to be provided under any resulting contract constitute a "bundle" pursuant to any rulings issued by the CRTC, to seek approval to provide these services and products.

h) A period of time has been allotted for bidders to complete any necessary processes with the CRTC. However, the time allowed for these processes must also be consistent with Canada and the client's operational requirements. The Contracting Authority will only grant extensions that it considers compatible with these operational requirements.

i) If, during the evaluation period, Canada proceeds to consider the next-ranked bidder under Subsection (e)(v) above, it may request that all remaining compliant bidders extend the validity periods for their bids, if applicable. Bidders will have no obligation to extend the validity periods of their bid. However, Canada will only continue to consider bids that remain valid for acceptance.

6.7 Regulatory Forms for Telecommunications Procurements

a) If indicated in the solicitation, bidders are requested to submit these regulatory forms with their bids on or before the closing date. If a bidder has not included any required regulatory form or has not, in the Contracting Authority's view, completed the form properly, the Contracting Authority will provide the bidder with an opportunity to submit the forms during the evaluation period. If the bidder does not submit the forms within the period set by the Contracting Authority, its bid will be declared non-compliant.

b) If different services or products proposed by the bidder are subject to different regulatory circumstances - for example, if some services or products are non-regulated or forborne, some services or products are subject to existing tariffs, and some services or products are proposed to be subject to new or amended tariffs - the bidder is required to submit Regulatory Forms A, B and C and specify which services or products fit into each of these categories. Given that the CRTC regulates different suppliers in different ways, this certification is required from each member of any joint venture bidder.

6.8 Regulatory Form A

Regulatory Form A
Regulatory Certification for Bids including Non-regulated or Forborne Services or Products

By submitting a bid, the bidder certifies that, on closing date, the services, products and prices proposed to Canada in this bid are not subject to any existing tariff and, to the best of the bidder's knowledge, based on an examination of all the information available to it on the closing date, the bidder is not required to submit any tariff to the CRTC to provide the services or products to Canada at the prices proposed.

This Certification applies to the following services and products:

_____
(*add more space as required*)

6.9 Regulatory Form B

Regulatory Form B
Regulatory Certification for Bids made under Existing Tariffs

By submitting a bid, the bidder certifies that it has submitted a complete and true copy of all existing tariffs that apply to the services and products described in its bid. The bidder also certifies that:

a) on the closing date, the services, products and prices it has proposed are in full compliance with the tariffs that apply and, to the best of the bidder's knowledge, based on an examination of all the information available to it on the closing date, it is not required to file any additional tariffs or amendments to provide these services and products at these prices;
b) the tariffs that apply do not include any rate ranges and all prices in the tariffs are firm (meaning they will not change during the contract period); and
c) it will immediately provide to the Contracting Authority any amendments made to these existing tariffs before contract award.

This Certification applies to the following services and products:

_____
(*add more space as required*)

6.10 Regulatory Form C

Regulatory Form C
Regulatory Certification for Bids made under Tariffs not yet approved by the Canadian Radio-television and Telecommunications Commission

By submitting a bid, the bidder certifies that it has submitted a complete and true copy of all proposed new tariffs (or all the existing tariffs that apply and the proposed amendments to those tariffs) that apply to the services and products described in its bid. The bidder also certifies that:

a) the proposed new tariff (or the existing tariff and the proposed tariff amendment) was submitted to the CRTC for approval before the closing date;
b) the tariffs that apply do not include any rate ranges and all prices in the tariffs are firm (meaning they will not change during the contract period); and

c) on the closing date, the services, products and prices it has proposed are in full compliance with the proposed new tariffs (or amended tariffs).

This Certification applies to the following services and products:

_____
(*add more space as required*)

6.11 Regulatory Form D

This form is required only after the closing date if the bid is based on a new or amended tariff - see the section of Part I, Evaluation Procedures for Bids based on a Draft Tariff. For a bid made by a joint venture, this certification would be required from each member of the joint venture bidder that submitted a tariff to the CRTC for approval.

Regulatory Form D
Post-Bid-Closing Regulatory Certification regarding Approval of New or Amended Tariffs

The bidder certifies that it has submitted a complete and true copy of all the new or amended tariffs, in the form approved by the CRTC on an interim basis, that apply to the services and products described in its bid. The bidder also certifies that:

a) the services, products and prices it has proposed are in full compliance with the new or amended tariffs, as approved by the CRTC on an interim basis, and do not, to the best of the bidder's knowledge, based on an examination of all the information available to it on the date set out below, require that any additional tariffs or amendments be filed;
b) it has identified in writing to the Contracting Authority all changes made to the version of the Draft Tariff originally submitted with its bid;
c) it will immediately advise the Contracting Authority regarding the final approval status of the Draft Tariff; and
d) if the Draft Tariff is further amended as part of the CRTC approvals process, the bidder understands that it must immediately provide those amendments to the Contracting Authority.

This Certification applies to the following services and products:

_____
(*add more space as required*)

Signature of the bidder_____
Print Name of the bidder_____
Print Title of representative of the bidder_____
Date Signed_____

Shared Services Canada

Conferencing & Operator Assisted Service (COAS)

Annex A - General Statement of Work

Version 1.0

Table of Contents

1 OVERVIEW

1.1 Introduction

(1) Shared Services Canada (SSC) requires an enterprise Conferencing & Operator Assisted Service (COAS) which will be referred to as the COAS Services, and provides the following to SSC and Clients:

a) SaaS Audio/Web Conferencing Services (AWS) as specified in Annex B;

b) Operator Assisted Service (OAS) as specified in Annex C; and

c) COAS Related Toll Free Services as specified in Section 2.

(2) SSC requires a Service Portal which will be a Web Portal consolidated on a single website. The Service Portal will become the primary point for e-communication between Canada, Clients and the Contractor providing:

a) COAS Services;

b) User Management;

c) Documentation, deliverables, reports and billing;

d) Service Management; and

e) Service Readiness.

1.2 General

(3) The COAS Service must provide self-serve on-demand conferencing needs accessible domestically and internationally to approximately 180 Government Departments, Agencies and Crown Corporations serving Canadians and Canadian interests.

(4) COAS Services must be a fully redundant technology (i.e., licenses, processes, and technology) to the existing MS-Teams Services deployed at Canada. The Contractor must provide COAS Services that in no part reuses the MS-Teams services already in use by Canada.

(5) Currently, SSC's conferencing application platforms are Microsoft Teams and Canada Conferencing Services (CCS) contract deploying the Webex application platform for audio/web conferencing services. Although the above conferencing application platforms account for approximately 80%, there are departments using other conferencing application platforms e.g., Zoom, Adobe Connect, Citrix Go-to Meeting.

(6) Currently, SSC's Operator Assisted Service is being delivered under the Government Teleconferencing Service (GTS) Contract.

(7) The Contractor must provide a fully managed cloud Software as a Service (SaaS) Platform to deliver AWS.

(8) The SaaS platform must require no hardware or software infrastructure be installed by Canada. Any exceptions to this requirement would require prior approval by the Technical Authority (TA) or delegate.

(9) The SaaS platform must be scalable to meet the AWS Peak Capacity as defined in Annex B and OAS Peak Capacity as defined in Annex C without impacting quality of COAS Services.

(10) The COAS Service and Service Portal must be available and accessible 24 hours per day, 7 days per week and 365 days per year with the exception of pre-approved planned Change Management maintenance windows.

(11) The COAS Service must be compliant with the Official Languages Act, the Accessible Canada Act, and COAS security requirements.

(12) The Contractor must provide a meeting banner for each AWS Conference and OAS (if applicable). The banner must include the department name or acronym of the Subscriber and the meeting title.

2 COAS Related Toll Free Services

(13) Toll-free numbers must allow a Participant to use COAS Services through the Public Switched Telephone Network (PSTN) without being directly charged.

(14) COAS Toll-Free numbers nationally will be provided by Canada during the Operational Readiness Phase for access to COAS Services for all participants. The Contractor must specify the method of communicating toll-free numbers to participants in the System Requirement Specification (SRS).

(15) The Contractor must not charge Canada for COAS Toll-Free usage.

(16) The Contractor must provide local numbers nationally and internationally for Participants to access COAS Services within 80 FGWDs after Contract Award. The Contractor must specify the method of communicating local numbers to participants in the System Requirement Specification (SRS).

3 SERVICE PORTAL

(17) The Contractor must provide a Service Portal as a central point of communication for COAS Services and Service Management that is accessible through the Internet.

(18) The Service Portal must have a scalable architecture to allow capacity for up to:

a) 10,000 concurrent sessions; and

b) 250,000 Service Portal users.

(19) The Contractor's Service Portal must use the WET Government of Canada Intranet theme version 4.0 or later and specified in the SRS. All pages (including Splash page) and branding must be provided as a wireframe in the SRS and approved by the TA (or delegate) as the *look and feel* of the COAS Service Portal.

(20) The Contractor's Service Portal must be designed to minimize number of clicks for the most common tasks (e.g., creating Service Requests (SR) and Incidents) allowing the Portal's performance to be user friendly and efficient to use.

(21) The Contractor must provide Canada a pre-production environment for the Service Portal (i.e., Staging) that mimics the production environment. Pre-Production will be used for:

a) user acceptance testing (UAT) during Operational Readiness;

b) UAT of new changes and releases;

c) UAT of foundational data bulk loading; and

d) Canada training purposes.

(22) The Contractor must copy production data (e.g., Service Requests, Incidents, etc.) to the pre-production environment within 3 Federal Government Working Days (FGWD) of a request from the TA (or delegate) at no cost to Canada.

(23) Service Level Targets and credits are not applicable for the Pre-Production Environment, but Incidents and problems must be remedied.

(24) The Contractor must provide a banner, with text approved by the TA (or delegate) in the Service Portal, to inform Users of:

a) any impacting COAS Service issues (e.g., planned maintenance windows, Incidents, service upgrades);

b) Privacy notice; and

c) Security notice.

(25) The Contractor must provide the TA (or delegate) pre-approved Quick Reference Guide, the Quick Reference Guide is a series of brief (less than 5 minutes) pre-recorded video training sessions in English and French that is accessible to Users on the Service Portal for the following topics:

a) User Profile management;

b) Service Requests;

c) Incident Management;

d) reports and billing;

e) User Management; and

f) All features and functions of the COAS Services.

(26) The Service Portal must use data validation for foundational data (e.g., FGWD calendar, Clients / Partner Government Organizations, Financial and Billing Codes, etc.) and must limit free text fields for user input. All free text fields must be specified in the SRS and approved by the TA (or delegate).

(27) The Contractor must enable bulk loading of data defined as foundational data by the TA (or delegate). Any foundational data must be supplied and verified in a pre-production environment by the TA (or delegate) before porting to the production environment.

(28) The Contractor must load, refresh, add, or change foundational data provided by Canada upon request from the TA (or delegate).

(29) The Contractor must provide the Service Portal and all requirements with a single sign-on authentication.

(30) Any part of the Service Portal requirements that are provided by third-party software or OEM tools must be specified in the SRS and approved by the TA (or delegate).

(31) The Contractor must provide all content in the Service Portal in the user's language of preference as specified in the User Profile or as selected on the Splash Page and must be persisted through the user's session.

(32) The Contractor must provide the capability in the Service Portal for the user to toggle between English and French after logon. The newly selected language must be persisted through the remainder of the session.

(33) The Contractor's Service Portal must provide auditable fields in the SRS. For data fields specified as auditable fields, the Service Portal must register all changes to the data including:

a) date and time when the change was made;

b) the previous value;

c) the new value; and

d) user's first and last name that affected the change.

(34) The Contractor's Service Portal must provide a history of the Service Requests including all interactions with the Contractor and Users. The accounting of interaction types must be specified in the SRS.

(35) The Contractor's Service Portal must provide a help section accessible to all users that is searchable and adheres to the Accessible Canada Act and the Official Languages Act. The help section must provide adequate information to use all features of the Service Portal, Service Management, Service Level Targets and COAS Services. The help section and Quick Reference Guide material must be specified in the SRS.

3.1 Software Requirements

(36) The Contractor's Service Portal must be accessible by the User without requiring a software application to be installed on:

a) Windows desktop;

b) Laptop device;

c) Mobile device; and

d) Tablet device.

(37) The Contractor must specify in the SRS and obtain TA (or delegate) approval for the browsers and versions the Contractor's Service Portal supports. The following browsers are used by Canada:

a) Chrome;
b) Safari;
c) Firefox; and
d) Edge.

(38) The Contractor must ensure that any software (such as plug-ins, add ins, applets), barring security limitation imposed by GC systems, that are necessary for devices to use the COAS Services:

a) are downloaded or available for download, installed and configured without requiring any actions other than responding to dialog boxes;
b) does not require the use of Adobe Flash or third party software; and
c) can be used without requiring the participant to have device administrative rights.

3.2 User Management

(39) The Contractor's Service Portal must provide User Management, defined as, managing user access to various components of the Service Portal and COAS Services. User management must consist of a strong RBAC for separation of data, roles and duties of users.

3.2.1 Role Based Access Controls

(40) The Contractor's Service Portal must allow one or more roles and associated permissions to be assigned to Service Portal user's "User Profile".

3.2.1.1 Roles and Permissions

(41) The Contractor must provide the following roles at a minimum:

a) Subscriber;
b) Technical Authority (TA);
c) Report Administrator (RA); and
d) Delegated Administrator (DA).

(42) A "Subscriber" means a role that must have the following permissions at a minimum:

a) Authorizes login to the Contractor's Service Portal; and
b) Authorizes their User Profile management (but cannot modify roles in User Profile).
c) search/read/view/download summary of their active/completed Service Requests;
d) creating, modifying or cancelling their Service Requests;
e) deactivate their account;
f) download their attended meeting recording(s) and transcript(s);
g) download their Post COAS Services Conference Summary Report;
h) report and create Incidents that requires Contractor's intervention; and
i) search/read/view/download summary of their active/closed Incident Tickets.

(43) A "TA" means a role that must have the following permissions at a minimum:

a) Add or change foundational data (i.e., Government(s) and Corporate Organization(s) and attributes);
b) Administer Electronic Billing Detail File (EBDF) and invoices;
c) query, sort and view Service Portal accounts and download results (i.e., CSV);

d) manage permissions (e.g., read, delete, download) per Service Portal user of the Document Management System (DMS);

e) add / remove permitted email domains;

f) query, sort and view all Service Requests and download results (i.e., CSV);

g) query, sort and view all Incidents and download results (i.e., CSV); and

h) view and download EBDF and all invoices;

(44) An "RA" means a role that must have the following permissions at a minimum:

a) Access to the DMS.

(45) A "DA" means a role that must have the following permissions at a minimum:

a) Assign roles to User Profiles;

b) Assign Billing accounts to User Profiles; and

c) Administer the following roles to users: TA, DA, and RA.

(46) The Contractor can expand and define additional permissions and roles to meet the Contractor's implementation requirements of the Contractor's Service Portal, role and organizational needs of COAS. Permissions and roles must be specified in the System Requirements Specification (SRS) and must be approved by the TA (or delegate).

3.2.1.2 Registration

(47) The Contractor's Service Portal must provide for self-registration for user's that includes collection of the following information for their User Profile creation at a minimum:

a) username (email address);

b) contact information including first and last name, email address and telephone number;

c) language preference (English, French);

d) Government organization name;

e) Government organization type (e.g., Client or Partner); and

f) Billing information (e.g., financial coding, billing address and billing contact information).

(48) The Contractor's Service Portal must provide the following information upon request for each User Profile:

a) status (Active/In-Active);

b) number of days in status;

c) creation date;

d) activation date (initial);

e) deactivation date; and

f) reactivation date (latest).

(49) Any other data collection or fields for self-registration must be specified in the SRS and must be approved by the TA (or delegate).

(50) The Contractor's Service Portal must filter email addresses domains for self-registration. The Service Portal must allow the TA (or delegate) to add / remove permitted email domains, if and as required.

(51) The Contractor must send an email for validation to the Service Portal user's email address. Once a User Profile has been verified, the user must provide a password for Service Portal access.

(52) The Contractor's Service Portal must allow for only the DA role to add new Client Organizations and billing data attributes.

(53) The Contractor's Service Portal must allow only the individual with the role of DA to:

a) Approve User Profiles; and

b) Assign role(s) to User Profiles.

(54) The Contractor's Service Portal must allow users to self-manage forgotten, expired or changed passwords by the Contractor sending an email verification request for existing accounts.

(55) The Contractor must allow any temporary passwords to have a minimum 5 day period before expiration.

(56) The Contractor must accept generic accounts, on an exceptional basis when User Profiles must contain generic information, for privacy and security reasons, and must be approved by the TA (or delegate).

(57) The Contractor's Service Portal must deactivate user access in the following ways:

a) a user can deactivate their own access;

b) accounts that have been inactive for greater than 90 days; and

c) the individual(s) with the DA role can deactivate any account at any time.

(58) When user access is deactivated the Contractor's Service Portal must send an email to the user with a notification that includes:

a) date of deactivation; and

b) instructions on how to re-activate their access.

3.3 Documentation Management System (DMS)

(59) The Contractor's Document Management System must have permissions to allow only RA roles access. Permissions must include at a minimum, download, delete and upload files.

(60) The DMS folder permissions must be managed by the TA (or delegate) role only.

(61) The Contractor must specify the DMS Structure and permissions in the SRS.

(62) The Contractor must specify file types for all DMS documents (e.g., Excel, Word, CSV) in the SRS.

(63) The Contractor must mock up and specify all DMS file content (e.g., file types, layout and structure) in the SRS.

(64) The Contractor must ensure that all DMS documents developed by the Contractor is kept current and up-to-date.

(65) The Contractor's DMS must be a repository for all documents detailed in the Contract, including at a minimum:

a) Service Portal reports;

b) Capacity reports;

c) master log of all Change Requests;

d) master log of all Problems;

e) Release Notes;

f) EBDF (reference);
g) per Client Summary Invoices;
h) SSC / Partner Summary Invoices;
i) Service Management issues log;
j) Contract Management issues log; and
k) Operational Readiness documentation;

3.3.1 Service Portal Report Management

(66) The Contractor's Service Portal must allow Service Portal reports to be downloaded in either Excel or CSV format.

Report Name	Service Management Report
Purpose	A summary of all required Service Management data
Frequency	Monthly - 5 FGWDs after the end of the month
roles	TA role
Language	English
Access	Service Portal DMS
Description	The report must include all data for providing Canada status on the health of Service Management including: a) Event and Incident Management; b) Change Requests; c) Service Requests; d) Problem Management; e) Capacity Management; f) Release Management; g) action items log since the previous meeting; and h) issues log from and since the previous meeting.

Report Name	Contract Management Report
Purpose	A summary and agenda for the Contract Management Meeting
Frequency	Monthly - 7 FGWDs after the end of the month
roles	TA role
Language	English
Access	Service Portal DMS
Description	The report must include all data for providing Canada status on the health of Contract Management including: a) a review on any issues or areas for improvement in the Contract; b) Contract issues requiring resolution; c) Service Catalogue updates; d) conferencing technology roadmap including emerging feature, services and trends;

	e) any issues not resolved at the Service Management Meeting; f) any other agenda item identified by the Contractor, TA or CA; and g) item tracking for Contract Amendment(s).

Report Name	Financial Summary Report
Purpose	A financial summary of all contract expenditures
Frequency	Monthly - 8 FGWDs after the end of the month
roles	TA role
Language	English
Access	Service Portal DMS
Description	The report must include all data for providing Canada status on the financial health of the Contract including: a) total contract expenditures; b) total monthly contract expenditures per Client; c) total contract year to date expenditure per Client; d) total monthly contract expenditures; and e) total contract year to date expenditure.

Report Name	Service Level Failure and Credit Report (SLFCR)
Purpose	A summary of all SLT Failures
Frequency	Monthly - 5 FGWDs after the end of the month
roles	TA role
Language	English
Access	Service Portal DMS
Description	The report must include all data for providing Canada the ability to monitor Service Level Targets and health of the Contract including: a) unmodified data used to calculate the actual SLT (e.g., Incident Ticket#, Incident reported time, Incident resolved time, etc.); b) calculated data to measure the actual Service Level Target Failure (e.g., outage time); c) SLT threshold; d) credit due per SLT failure; e) SLT credit exemption(s) provided by Canada; and f) total Service Credit due on next invoice and EBDF.

Report Name	Capacity and Performance Report
Purpose	The Contractor must design and monitor Key Performance Indicators (KPIs) that must accurately reflects the quality and performance over time of: a) COAS Services; and b) Service Portal.
Frequency	Monthly - 5 FGWDs after the end of the month
roles	TA role
Language	English
Access	Service Portal DMS
Description	The report must include all data for providing Canada status on the health of the COAS Services and Service Portal Capacity: a) unmodified data used to calculate KPI; b) calculated data to measure the actual KPI; c) capacity threshold(s); and d) capacity recommendations and upgrades.

Report Name	Post COAS Services Conference Summary Report
Purpose	A summary of the COAS Services Conference details for each audio/web conference.
Frequency	Per conference (upon completion)
roles	Subscriber (for their conferences)
Language	Bilingual (English and French)
Access	Portal (accessible for 60 days after conference ended)
Description	The report must include: a) conference type (i.e. Webcast, Audio Only, Audio/Web Conference, Operator Assisted); b) subscriber name; c) Government Organization name; d) conference identifier; e) Participant connection details (identifier, connect and disconnect times, phone number, etc.); f) meeting time (e.g. start time, end time, duration, etc.); and g) number of participants.

3.4 Service Requests (SR) for OAS

(67) The Contractor's Service Portal must allow Subscribers to create, change, or cancel a SR through:

a) Service Portal Web Form; and

b) Calling the Service Desk.

(68) The SR web form must be specified in the SRS and at a minimum include all features specified in the Annex C (Operator Assisted Services) and the OAS tab of the Pricing Table (Service Catalogue).

(69) The Contractor must provide SR Acknowledgement Notification to the Subscriber to acknowledge creation, changes, or cancellations of SRs within 1 hour of request.

3.5 Service Requests (SR) for AWS

(70) The Service Portal must allow Subscribers to create, change, or cancel a SR for Audio / Web Conferencing through:

a) Service Portal Web Form;

b) Calling the Service Desk;

c) OEM interface; and

d) Outlook extensions.

(71) The Contractor must specify the SR web form in the SRS and at a minimum include all features specified in the Annex B (Audio Web Conferencing Service) and Audio Web Tab of the Pricing Table Service Catalogue).

(72) The Contractor must provide SR acknowledgement notification to the Subscriber to acknowledge creation, changes, or cancelations of SRs within 5 minutes of request.

3.6 Recording Management

(73) The Contractor's Service Portal must allow a Subscriber to manage audio/web and operator assisted conference recordings that they scheduled or requested that includes:

a) searching for recordings by selected filters including: scheduled date, scheduled time, meeting subject, meeting title, contact name (primary, secondary), and identifier;

b) sharing / downloading selected recording(s) in a non-proprietary format (i.e., MP3 or MP4) as selected by the Subscriber; and

c) deleting one or more recordings where the Subscriber is requested to confirm the deletion request prior to the deletion of the recording(s).

3.7 Service Portal Incidents

(74) The Contractor's Service Portal must allow Subscribers to create Incident tickets in the Service Portal.

(75) The Contractor must specify the Incident web form in the SRS and at a minimum include all required data fields for the Contractor to resolve Incidents.

(76) The Contractor must provide Incident Acknowledgements to the originator to acknowledge creation, changes, or cancelations of Incidents within 15 minutes of request.

3.8 Searching

(77) The Contractor's Service Portal must allow the following to be searchable:

a) users (for DA role only) including:

i) user last login date and time; and

ii) user deactivated date.

b) all SRs (for TA role only);

c) SRs for logged in Subscriber;

d) all Incidents (for TA role only);

e) Incidents for logged in Subscriber; and

f) help section (if required).

(78) The Contractor must allow all data fields for SR, User Profiles, and Incident tickets to be searchable, exceptions must be approved by the TA (or delegate).

(79) The Contractor must allow all data fields to be displayed in search results, exceptions must be approved by the TA (or delegate).

(80) The Contractor must allow all search results to be downloaded in CSV format.

3.9 Notifications

(81) The Contractor must provide notifications in bilingual format or sent in the Preferred Language of the user.

(82) The Contractor's Service Portal must allow users the option to subscribe and unsubscribe to notifications based on their role. Default notification subscriptions per role must be specified in the SRS.

(83) Where action (e.g., approval, resolution, participation) is required of Canada, the Contractor must send a notification to the appropriate user (e.g., originator, TA, etc.).

(84) The Contractor's Service Portal must send a registration approval notification to the user that includes:

a) Verifying access has been granted;

b) URL for contact information for Service Desk;

c) URL for Service Portal; and

d) URL to access a Quick Reference Guide.

(85) The Contractor must provide acknowledgment notifications to the originator for creation, changes and updates to the following:

a) Incident tickets; and

b) SRs.

(86) The Contractor must provide notifications to a configurable recipient list as provided by the TA (or delegate) for the upload of the following:

a) Service Portal reports;

b) EBDF;

c) Summary Invoices (per Client); and

d) Aggregated SSC / Partner Summary Invoices.

4 SERVICE MANAGEMENT

(87) Service Management is the Contractor specialized organizational capabilities for enabling, operating and managing the lifecycle of COAS Services.

(88) Service Management must start once Operational Readiness Phase is complete or as approved by the TA (or delegate) and continue during the Operations Phase or until contract termination.

(89) The Contractor must use their standard operating procedures as full IT lifecycle management for Service Management, the Service Portal and COAS Services to ensure availability, integrity and resiliency.

(90) The Contractor must incorporate ITIL principles for the Services, as described in the following subsections.

4.1 Service Management Resources

(91) The Contractor must provide an experienced Service Manager knowledgeable with conferencing technology services to act as the single point of contact with the TA (or delegate) and to be responsible for all Service Management issues including:

a) represent the Contractor regarding all issues related to Contract management, COAS Services, Service Management or Service Portal Issues;

b) represent the Contractor to address any escalations (e.g., technical, outages, Incidents, administrative, billing, etc.);

c) coordinate activities in conjunction with the Contractors subject matter expert(s);

d) must be available to meet with the Technical Authority (or delegate) when and as requested by either party; and

e) facilitate periodic Operations Management Meetings (e.g., bi-weekly, monthly, ad-hoc, as required).

(92) The Contractor must provide to Canada at no additional charge any other personnel that is required to support Canada in any aspect of Service Management, COAS Services or the Service Portal.

4.2 Change Request (CR)

(93) The Contractor acknowledges that a Change Request is a request, originating from the Contractor or Canada to:

a) request changes to the Service portal;

b) request changes to COAS Services; and

c) request changes to Service Management.

(94) The Contractor must respond with a description for the recommended Change and provide costs of a Change Request to the TA (or delegate) within 10 FGWDs.

(95) The Contractor acknowledges that a Change Request type “Service Portal Feature Change” is a change that requires a full Service Release Cycle to implement. A Change Request is permitted to take longer than one (1) Service Release Cycle if approved by the TA (or delegate).

(96) The Contractor acknowledges that a Change Request for a “Standard Change” is any change requiring less than a full release cycle. Standard Changes must include the following common changes, at a minimum:

a) report output changes (e.g., aesthetics, adding / removing fields, rows or columns, field label changes, output format and syntax, minor calculation changes, etc.);

b) Loading, adding or refreshing Foundational Data; and

c) Web form changes (e.g., aesthetics, new fields, removing fields, changing a label, making a field optional / mandatory, minor calculation changes, making fields auditable / not auditable, etc.)

(97) The Contractor must provide a cost breakdown and substantiation of cost for the proposed change in sufficient detail for the TA (or delegate) to approve the Change.

(98) The Contractor must complete the Change Request activity in maintenance windows approved by the TA (or delegate). Any exceptions must be approved by the TA (or delegate). Maintenance windows are not considered outage time for SLT monitoring.

(99) The Contractor must open an Incident ticket in order to track any outage time related to a Change outside the approved maintenance window.

(100) The Contractor must create and maintain a master log of Change Requests.

(101) The Contractor must allow the TA (or delegate) to perform UAT in a non-production environment before porting change to production environment.

4.3 Service Release Management

(102) The Contractor acknowledges that a Service Release is defined as:

a) Change not requested by Canada to the Service Portal or COAS Services;

b) OEM software, hardware or firmware patching or updates; and

c) Security patching or updates.

(103) The Contractor must use Change Management for any Service Releases to the Service Portal or COAS Services.

(104) The Contractor must keep COAS Services patched and up to date as per all OEM's recommendations.

(105) The Contractor must provide Release Notes which document details of any Service Releases and must detail any changes to user experience, at a minimum. Release Notes must be posted to the Service Portal prior to porting into production environment.

(106) The Contractor must test all Service Releases in the non-production environment before porting a change to the Production environment.

(107) Service Releases that change user experience must obtain TA (or delegate) approval through testing in the non-production environment prior to porting to the production environment.

4.4 Service Request (SR)

(108) The Contractor must provide a Subscriber the full self-serve ability to create, modify or cancel SRs for Audio / Web Conferencing Services through:

a) Service Portal;

b) Locally installed OEM Software (e.g., desktop applications, Calendar plug-ins, etc.) as per Annex B; and

c) Calling the Service Desk.

(109) The Contractor must provide a Subscriber the full self-serve ability to create, modify or cancel SRs for OAS Services through:

a) Service Portal;

b) Calling the Service Desk.

(110) The Contractor must create and maintain all SRs in the Service Portal independently of how it was requested.

(111) The Contractor's Service Portal must provide SR history which includes:

a) SR action taken;

b) user and Contractor personnel who took the action; and

c) time and date of action.

(112) The Contractor must provide notifications to acknowledge creation, changes, or cancelations of SRs to the originator within 5 minutes.

4.5 Event and Incident Management

(113) The Contractor must proactively monitor the health of COAS Services and the Service Portal through "Event Management".

(114) The Contractor acknowledges that Incident Management are issues reported either by the originator or the Contractor that impact Service Management, Service Portal or COAS Services.

(115) The Contractor must maintain all Incident Tickets in the Service Portal independently of how the Incident was reported.

(116) The Contractor must allow the originator to report an Incident by:

a) Creating an Incident ticket on the Service Portal;

b) * touch command from a telephone;

c) In Conference chat; and

d) calls to the Service Desk.

(117) The Contractor must notify the originator when the Incident is created, provide ongoing worklog updates, and when the Incident is completed. The Contractor must validate that the Incident has been fixed with the originator before closing an Incident Ticket.

(118) The Contractor must create an Incident Ticket for any Event that may impact COAS Services.

(119) The Contractor must provide AWS testing tools to diagnose originator's network issues at the time the Incident is being reported. Incidents that are caused by the originator's network are not treated as an Incident. The testing tools and triage process must be included in the SRS.

(120) The Contractor must create an Incident Ticket that includes enough information to:

a) Provide status and resolve Incidents;

b) Identify outage time (from identification to service restoral);

c) manage SLTs;

d) identify impacts of Incident;

e) identify Root cause of Incident; and

f) manage the tasks and status of an Incident until resolved (e.g., worklog).

(121) The Contractor must work to resolve Incidents with the originator and any other parties, if and when required.

(122) The Contractor must categorize and assign Incidents with a priority (i.e., high, medium, low) as approved by the TA (or delegate).

(123) The Contractor must notify the TA (or delegate) of any Major Outages or any Incident escalations.

(124) An Outage is an interruption rendering the full Service or parts of the Service unavailable. The Contractor must communicate all Major Outages to users as:

a) a Service Portal banner; and

b) a Service Desk recorded announcement.

(125) Outages are classified as major or minor as follows:

a) **Major Outage:** The Contractor must classify Incidents and events as Major when:

i) multiple conferences are affected;

ii) any portion of the COAS Services are inoperable to more than 1 user;

iii) any portion of the Service Portal are inoperable to more than 1 user; and

iv) COAS Services are severely degraded for more than 1 conference.

b) **Minor Outage:** The Contractor must classify Incidents and events as Minor when:

i) unexpected termination of a single conference while in progress;

ii) any severe degradation in the performance of the service connection that would render a single in-progress conference session unusable;

iii) the unexpected disconnection of a Participant, including an Operator, in a conference; and

iv) any unexpected system disruption or delay in the start of a scheduled conference that cannot be accommodated or re-started within 5 minutes of the scheduled start time.

(126) The TA (or delegate) may approve to exclude a portion or all Outage time for the Incident or Event during a review of the Incidents during the Service Management Meeting provided the Contractor provides all data to support that the Incident will not be reoccurring.

4.6 Problem Management

(127) The Contractor must pro-actively identify, investigate, diagnose, analyze (trend) and correlate Incidents and Events in order to determine Problems.

(128) The Contractor must designate 3 or more Incidents with the same root cause within a rolling 90-day window as a Problem. Problems must be resolved through Change and / or Release Management.

(129) The Contractor must register a Problem upon request from the TA (or delegate) for any non-Incident type issue that impacts the following:

a) COAS Services;

b) Service Portal; and

c) Service Management.

(130) The Contractor must manage Problems through to resolution, ensuring that root cause is determined, preventive measures are implemented, and appropriate "clean-up" is done to remedy the Problem quickly.

(131) The Contractor must maintain a Problem Management Log (updated monthly at a minimum) and present in the Service Management Meeting that includes for all Problems:

a) Problem identifier;

b) Dates (i.e., opened, closed, cancelled); and

c) actions / tasks / next steps to remediate the Problem including;

i) who is responsible; and

ii) due date.

4.7 Capacity and Performance Management

(132) The Contractor must engineer and design the COAS Services and the Service Portal which includes, but not limited to:

a) reviewing and analyzing COAS Services quality and performance;

b) adapting, tuning, and improving COAS Services to ensure optimal performance;

c) proactively assessing against Peak Capacity for Services; and

d) advising the TA (or delegate) when capacity thresholds are being exceeded and capacity upgrades are warranted.

(133) The Contractor must measure Capacity and Performance in the Capacity and Performance Report. The Key Performance Indicators (KPIs) must accurately reflect the quality and performance over time for:

a) COAS Services; and

b) Service Portal.

(134) The Contractor must update the Capacity and Performance Report monthly, at a minimum, and must upload to the DMS and must be presented to the TA (or delegate) at the Service Management Meeting.

4.8 Information Management

(135) The Contractor must not delete any Service Portal or COAS data without approval from the TA (or delegate), unless otherwise specified.

4.9 Service Desk

(136) The Contractor must provide a Service Desk in both of Canada's Official Languages, English and French, available 24 hours per day, 7 days per week, 365 days per year, which must be accessible to Participants by:

a) toll-free telephone number(s) (i.e., 1-8xx number);

b) local number(s) where applicable;

c) * touch command;

d) in conference chat; and

e) an email address.

(137) The Contractors' Service Desk staff must provide technical assistance, if required for any functions including self-serve for:

a) COAS Services;

b) Service Portal; and

c) Service Management.

(138) The Contractor must, provide an automated audio message in both of Canada's Official Languages (English and French) to advise users of Major Outages.

4.10 Escalation Management

(139) The Contractor must provide an Escalation Matrix 15 FGWDs after contract award.

(140) The Escalation Matrix is a roadmap regarding the order of contacts for Service Management and must include, at a minimum:

a) name of person at each level of escalation;

b) email and phone number for each level of escalation;

c) must include a minimum of 4 levels of escalation; and

d) the highest level of escalation must be a VP level.

(141) The Contractor must provide an Escalation Matrix for any issues related to the following areas of Service Management and Operational Readiness:

a) Release Management;

b) SRs;

c) Event and Incident Management;

d) Problem Management;

e) Capacity Management;

f) Service Desk;

g) Billing Management;

h) Service Portal Delivery;

i) Project Management for Operational Readiness;

j) SA&A Delivery; and

k) COAS Services Delivery.

(142) The Contractor must escalate issues according to the intervals described in the Escalation Matrix or requested by the TA (or delegate).

4.11 Billing Management

(143) The Contractor must provide summary invoices and EBDF for COAS Services on a monthly basis within 10 FGWDs at the end of the calendar month billing period.

(144) Annual license fees must be invoiced after In-Service is achieved and must be invoiced every 12 months afterwards.

(145) The Contractor Summary Invoices and an Electronic Billing Detail File (EBDF) for all billing periods must be accessible through the DMS.

4.11.1 Summary Invoices

(146) The Contractor must invoice COAS Services monthly as follows:

a) Annual License Fees for year 1 must be summarized on the SSC Summary Invoice;

b) COAS Services must be summarized per Client (Client Summary Invoice) on a single summary invoice and billed directly to each Client;

c) Annual License Fees must be summarized per Client (Client Summary Invoice) on a single summary invoice and billed directly to each Client Starting at contract year 2;

d) COAS Services must be summarized for Partners and SSC on a single summary invoice (SSC Summary Invoice) and billed directly to SSC;

e) Annual License Fees must be summarized for Partners and SSC on a single summary invoice (SSC Summary Invoice) and billed directly to SSC starting at contract year 2.

f) Other charges (e.g., Chargeable Change Requests, Milestone payments, Service Credits, etc.) must be included on the SSC Summary Invoice.

(147) The Contractor must deliver non-modifiable (e.g., pdf, hardcopy, etc.) summary invoices (e.g., mailed, emailed, etc.) to each Client's billing address.

4.11.2 Electronic Billing Detail File (EBDF)

(148) The Contractor must provide an aggregated electronic billing data format (EBDF) (i.e., comma delimited file format) that includes all charges for the given billing period via the Service Portal. The Contractor must provide a monthly (calendar month) EBDF file within 5 FGWD's following the end of the billing period. The Contractor acknowledges that the format of the Electronic Billing File must comply with the specifications in Appendix 2 – Electronic Billing File to Annex A.

(149) The Contractor must not make any changes to the EBDF without a Change Request approved by the TA (or delegate).

(150) The Contractor must provide a minimum of the following information in its invoice detail records for each conference:

a) Department identifier;

b) Department code;

c) Billing code;

d) Account name;

e) Reservation identifier;

f) Requested start time;

g) Cancel Time;

h) Username;

i) Username email address;

j) Conference type;

k) Conference title;

l) Conference date & time;

m) Connections reserved;

n) Connections actual;

o) Number of Operators reserved;

p) Number of actual Operators;
q) Minutes duration;
r) Base conference cost;
s) Each additional option feature;
t) Each additional option feature cost;
u) Number of Toll-Free minutes used;
v) Number of Toll-Free Subscribers;
w) Toll-Free per minute cost;
x) Toll-Free total costs;
y) Cancellation notice in hours;
z) Cancellation fees;
aa) Unused port charges (if applicable);
bb) Other charges pre-approved by Canada with description and cost;
cc) Total conference cost;
dd) EBDF – user, dept, # minutes;
ee) Number of used ports;
ff) Number of reserved ports;
gg) Subscriber name;
hh) Client or partner;
ii) start date of the OAS Conference;
jj) start time of the OAS Conference;
kk) end date of the OAS Conference;
ll) end time of the OAS Conference;
mm) duration of the OAS Conference;
nn) "billable" conference features used;
oo) Conference features used;
pp) Unique Meeting identifier;
qq) type of COAS Services Conference (i.e., Webcast, Audio/Web conference, Audio only and OAS);
rr) start date and time of the COAS Conference;
ss) end date and time of the Audio Conference;
tt) telephone number used (1-8xx, local);
uu) total number of minutes used;
vv) recording status (enabled, disabled);
ww) number of minutes Audio Conference Operator participated (Scheduled Audio Conferences only);
xx) Audio Conference Access Code or reservation number;
yy) total number of Participants;
zz) duration of the Audio Conference;
aaa) Total monthly minutes;

bbb) number of individual conferences;

ccc) start date of the Web Conference;

ddd) start time of the Web Conference;

eee) end date of the Web Conference;

fff) end time of the Web Conference;

ggg) duration of the Web Conference;

hhh) identifier of the Web Conference (i.e., session id); and

iii) total number of Participants.

4.12 Operations Management Meetings

(151) The Contractor acknowledges that Operations Management Meetings are to commence the month after Operational Readiness is complete or as requested by the TA (or delegate).

(152) The Contractor acknowledges that following recurring mandatory meetings must be scheduled for the Operations Phase and must include at a minimum:

a) Monthly Service Management Meetings; and

b) Contract Management Meetings (as specified by the Contract Authority (CA) or delegate).

4.12.1 Service Management Meetings

(153) The Contractor's Service Manager must host and ensure all Contractor's Subject Matter Experts (SMEs) are participating in the Monthly Service management Meeting at a time and date as approved by the TA (or delegate).

(154) The Contractor is responsible to issue a record of decision and update all reporting following each meeting within 5 FGWD's for review by either the Technical Authority and/or Contracting Authority (or delegates).

(155) The Contractor must provide the agenda and Service Management Report to facilitate and conduct the Service Management Meetings.

4.12.2 Contract Management Meeting

(156) The Contractor must organize and convene a contract review meeting as requested by the CA (or delegate).

(157) The Contractor must issue a record of decision and action register following each meeting within 5 FGWD's for review by either the Technical Authority and/or Contracting Authority (or delegates).

(158) The Contractor must prepare the agenda and Contract Management Report to facilitate and conduct the Contract Management Meeting.

5 OPERATIONAL READINESS

(159) The Contractor acknowledges that the Operational Readiness Period starts at Contract Award and continues until the Operational Readiness Period is complete or as approved by the TA (or delegate).

(160) All Operational Readiness deliverables must be uploaded to the Service Portal by the required dates and approved by the TA (or delegate).

(161) Any reiterations required to Operational Readiness deliverables, the Contractor must deliver and provide iterations within 5 FGWDs.

(162) Canada requires 5 FGWDs to review each Operational Readiness deliverable and either provide feedback to the Contractor, or approval.

5.1 Operational Readiness Resources

(163) The Contractor must provide a Project Manager as a single point of contact for the Operational Readiness period, at no additional cost to Canada. The Project Manager must collaborate with and obtain approval from the TA (or delegate) for all activities and deliverables necessary for COAS Implementation. For a successful implementation, the following activities, as a minimum, may be required:

a) Develop and maintain the Implementation Plan's completeness and accuracy;
b) Security Assessment and Authorization (SA&A) process;
c) Service Portal Delivery;
d) steering committees and Contract oversight;
e) any project management plan required to manage the delivery of Operational Readiness (e.g., risk, issue, change, HR management, etc.); and
f) Manage any escalations.

(164) The Contractor must provide the necessary personnel to oversee and coordinate all aspects of Service Implementation and Acceptance testing at no additional cost to Canada.

5.2 Implementation Plan and Milestones

(165) The Contractor must coordinate an initial kickoff meeting within 5 FGWDs with the TA and CA (or delegates) at a time and location scheduled by the Contractor to finalize the Implementation Plan.

(166) The Contractor's Implementation Plan provided with their bid response is subject to approval by the TA (or delegate) following contract award.

(167) The Contractor acknowledges that the Implementation Plan must include:

a) all tasks and milestones that includes:
    i) task description;
    ii) duration;
    iii) start and finish;
    iv) dependencies;
    v) resources; and
    vi) deliverables.

b) the Contractor's Governance structure (including all contact information of the Implementation team and SMEs);

c) the Contractor's Escalation Matrix; and

d) Operational Readiness Period Critical path.

(168) The Contractor acknowledges that SSC will be using the Implementation Plan for monitoring the Operational Readiness Phase. The Implementation Plan must include adequate detail for Canada to monitor status of the COAS Implementation. The Contractor agrees to enrich the plan with additional detail as requested by Canada.

(169) The Project Milestones as detailed in the Implementation Plan and any contingencies must not exceed any of the intervals in the Project Milestones from Table entitled Project Milestones.

(170) The Implementation Plan and all activities must be completed by June 30, 2024 or earlier.

(171) The Project Deliverables Milestones and Interval Table below states the project maximum intervals in FGWDs since Contract Award for milestones:

Project Milestones	
Interval (FGWDs since contract award)	**Milestones**
5	Project Kick Off Meeting
40	Service Portal Gate 1
85	Service Portal Gate 2
140	Service Portal Gate 3
50	SA&A Gate 1
100	SA&A Gate 2
140	SA&A In-Service
100	COAS Services Gate 1
140	COAS Services In-Service
140	Service Portal In-Service
145	Operations Phase

5.3 Service Portal Acceptance

(172) The Contractor acknowledges that the following Service Portal Gates must be adhered to as follows:

a) Service Portal Gate 1 is obtained when the final SRS is delivered to Canada for review and approval.

b) Service Portal Gate 2 is obtained when:

i) the SRS is approved by Canada; and

ii) the Service Portal pre-production environment access is provided to Canada for UAT testing.

c) Service Portal Gate 3 is obtained when:

i) UAT testing is complete and approved by the TA (or delegate);

ii) Major UAT defects remediated;

iii) Service Portal is fully functional and ported into Production; and

iv) Production access has been provided to the TA (or delegate).

5.3.1 Service Portal System Requirement Specification (SRS)

(173) The Contractor must provide a System Requirement Specification (SRS) for the Service Portal which specifies the Service Portal design, the user interface look and feel and use of COAS branding. The SRS must contain the following design specifications with bilingual user interfaces (English and French):

a) Service Portal Wireframes;

b) Service Portal processes;

c) Service Portal report samples;

d) All OEM or 3rd party software being used; and

e) Service Portal Notifications.

(174) Any questions or assumptions about SRS development must be directed to the TA (or delegate) prior to submission of the final SRS.

5.3.1.1 Service Portal Wireframes

(175) The Contractor must provide wireframes that:

a) are graphical representations of each Service Portal webpage;

b) provide functional elements of each webpage (e.g., actions to be taken from a page (buttons), fields and field labels, etc.); and

c) provide a design for Service Portal's structure (e.g., menus and menu structure), look / feel, and any use of branding.

(176) The Contractor must provide SRS Wireframes for all Service Portal pages for both English and French including at a minimum:

a) Splash page;

b) Home page;

c) SR create, change and cancel page(s) (including all fields for features or functions for ordering COAS Services);

d) SR search page(s) (including search filters);

e) SR search results page (including data fields / columns in results);

f) Incident Ticket create page (including all fields required to fix the Incident);

g) Incident Ticket search page (including search filters);

h) Incident Ticket search results page (including data fields / columns in results);
i) add / remove domain filter pages;
j) User Profile page;
k) Self-registration page;
l) RBAC management pages (e.g., adding roles to profiles, pending approval page, etc.);
m) Notification management pages (i.e., user subscription management);
n) DMS pages and folder structure;
o) DMS permission management pages;
p) Service Portal banners (e.g., personal information usage, security protection levels, etc.);
q) Standard error pages (i.e., page not found);
r) Server messages (e.g., logged off, server errors, etc.);
s) Help section pages; and
t) Recording and transcription management pages (e.g., search filters, search results, etc.).

(177) The Contractor's Service Portal Wireframes must include all data field specifications for all forms and pages with translations including:

a) Field Label;
b) Field Type and length (including free text fields);
c) Data validation (e.g., calendar, field masks, foundational drop down data, etc.); and
d) Auditable fields.

5.3.1.2 Service Portal Processes

(178) The Contractor's SRS must include all processes for the Service Portal including at a minimum:

a) User Management process;
b) SR process;
c) Incident Management process;
d) Billing Management process; and
e) Any other process to support Service Portal operations (e.g., Change Management, Release Management).

(179) The Contractor's SRS must include a Service Portal Process Diagram for all Service Portal processes including:

a) swim lanes including user roles;
b) Canada and Contractor tasks;
c) Actions (i.e., buttons) and / or states of the process;
d) Connections between states and / or actions; and
e) Triggers for notifications.

5.3.1.3 Service Portal Report Samples

(180) The Contractor must provide sample output reports as per the Section entitled "Searching".

(181) The Contractor must provide a mock up of all Service Portal reports (see Section Service Portal Report Management) in the SRS.

(182) The Contactor must provide sample Summary Invoices and EBDF in the SRS.

5.3.1.4 Service Portal Notifications

(183) The Contractor must detail in the SRS how notifications are limited to RBAC roles, and the options and the method(s) for users to subscribe and unsubscribe to notification(s) of their choosing.

(184) The Contractor must include all notification samples (i.e., emails) which must be mocked up in the SRS and must include:

a) Notification trigger;

b) Notification recipients;

c) Sender email address;

d) Subject text in both English and French; and

e) Message body text in both English and French.

5.3.2 Service Portal User Acceptance Testing

(185) The Contractor acknowledges that the Service Portal UAT must be performed in a pre-production environment prior to porting to the Production environment.

(186) The Contractor must provide Contractor-guided UAT (virtual or in-person) to ensure the Service Portal adheres to the SRS specifications. Any exceptions must be approved by the TA (or delegate).

(187) The Contractor acknowledges that Canada must be allowed to perform independent UAT of all Service Portal functions detailed in the SRS during the acceptance testing.

(188) The Contractor must fix any high impact defects from UAT testing prior to porting to Production and any fixes must be accommodated in the Project Schedule.

(189) The Contractor acknowledges that the TA (or delegate) must approve that the UAT Testing is thorough and complete. An Action Plan to remediate any outstanding defects must contain adequate level of detail to inform the TA (or delegate) of any risks with the Production port, must be accommodated in the Project Schedule, and must be approved by the TA (or delegate).

5.4 COAS Services Acceptance

(190) The Contractor acknowledges that the following COAS Service Gates must be adhered to as follows:

a) COAS Services Gate 1 is obtained when access is provided to Canada for UAT testing of COAS Services as described in Annex B.

b) COAS Services In-Service milestone is obtained when:

i. UAT testing is complete and approved by the TA (or delegate);

ii. Major UAT Defects remediated;

iii. COAS Services are fully functional and ready for Production; and

iv. Production access has been provided to the TA (or delegate).

(191) Authority to Operate (ATO) COAS services is contingent on approval of SA&A In-Service milestone.

5.4.1 COAS Services Acceptance Test Plan

(192) The Contractor must provide an Acceptance Test Plan for approval by the TA (or delegate). The Acceptance Test Plan should test, at a minimum, the following functionality:

a) All audio/web conferencing functions and features;

b) All OAS conferencing functions and features;

c) Performance experienced during live use of Operator Assisted scheduling;

d) Performance experienced during live use of Operator Assisted Services, and use of Service Desk support services; and

e) All Quick Reference material for COAS Services.

5.4.2 COAS Services UAT

(193) The Contractor must provide Contractor-guided COAS Services UAT (virtual or in-person) to ensure COAS Services adheres to the Annex B and Annex C and follows the COAS Services Acceptance Test Plan. Any exceptions must be approved by the TA (or delegate).

(194) The Contractor acknowledges that Canada must be allowed to perform independent UAT of all COAS Services detailed in Annex B and Annex C.

(195) The Contractor must fix any high impact defects from UAT testing prior to porting to Production and must be accommodated in the Project Schedule.

(196) The Contractor acknowledges that the TA (or delegate) must approve UAT Testing which is thorough and complete. An action plan to remediate any outstanding defects must contain adequate level of detail to inform the TA (or delegate) of any risks with COAS Services going live and must be approved by the TA (or delegate).

5.5 SECURITY ASSESSMENT & OPERATIONAL SECURITY

5.5.1 Security Assessment

(197) The Contractor must complete a First Party Security Assessment OR a Third Party Security Assessment as selected by the Contractor.

5.5.2 First Party Security Assessment

(198) The Contractor must complete Gate 1 Security Design and Gate 2 Security Design Validation where the Work for Gate 1 must be completed and accepted by Canada prior to the Work for Gate 2.

5.5.2.1 SA&A Gate 1: Security Design

(199) The Contractor must provide a Security Design that must include:

a) a high-level component diagram that clearly shows the Service architecture, the allocation of services and components to network security zones, and identifies key security-related data flows;

b) a description of the network zone perimeter defenses;

c) a description of the use of virtualization technologies, where applicable;

d) descriptions of the allocation of all technical security requirements to high-level service design elements at all architectural layers;

e) descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements;

f) allocation of the security requirements at each of the architecture layers of the high-level service design;

g) definition of the architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer);

h) a description of the approach for remote management;

i) a description of the approach for access control;

j) a description of the approach for security management and audit;

k) a description of the approach for configuration management;

l) a description of the approach for patch management;

m) justification for key design decisions; and

n) a description of how the following security functions will be implemented:

   i) access control;

   ii) security management and audit;

   iii) configuration management;

   iv) patch management; and

   v) remote management.

(200) The Contractor must provide a Security Requirements Traceability Matrix (SRTM) that contains the following information that provides evidence of conformities to the security control for each security requirement in Appendix 3 to Annex A: COAS SOW Security Requirements:

a) the security requirement (SR) identifier;

b) an identifier that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line identifier);

c) the security requirement statement;

d) a description of how the security requirement is addressed in the Security Design in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements;

e) the title of the Contract deliverable(s) in which the Contractor will provide the details of its security solution for the requirement (i.e., service continuity plan); and

f) tracing (a reference to an identifiable element) to the Security Design to allow Canada to confirm that the security safeguards satisfy the security requirements.

5.5.2.2 SA&A Gate 2: Security Design Validation

(201) The Contractor must provide an Integration Security Test Plan that must include:

a) the security functions to be tested;

b) Canada witnessing the testing arrangements; and

c) for each security function or sets of security functions, the items to be tested, including:

   i) a description of the test case, procedure, or scenario;

   ii) environmental requirements;

   iii) ordering dependencies; and

   iv) expected results (i.e., pass/fail criteria).

(202) The Contractor must conduct integration security testing in accordance with the Integration Security Test Plan and provide an Integration Security Test Report for each of the test items in the Integration Security Test Plan:

a) the expected results (i.e., pass/fail criteria);

b) the actual results; and

c) a description of deviations and how each was resolved.

(203) The Contractor must provide a Vulnerability Assessment Plan that must include:

a) a description of the scope of the vulnerability assessment;

b) Canada witnessing arrangements;

c) a description of the vulnerability assessment process; and

d) a description of the vulnerability assessment tools that will be used, including any software versions.

(204) The Contractor must conduct a vulnerability assessment in accordance with the approved Vulnerability Assessment Plan that includes:

a) a listing of the vulnerability assessment tests that were conducted;

b) all raw data for the results of the vulnerability assessment tests in a Commercial Off the Shelf (COTS) file format and names specified by Canada;

c) for each vulnerability assessment test:

i) whether a known vulnerability was detected;

ii) a description of the vulnerability; and

iii) a description of the patch or corrective measure that was implemented to resolve the vulnerability.

d) for any unresolved vulnerability:

i) an assessment of the significance of the vulnerability in the context of the Services; and

ii) the vulnerability identifier for the outstanding patch or corrective measure; or

iii) the rationale for not implementing a patch or a corrective measure.

(205) The Contractor must provide a Security Installation Verification Plan that must include:

a) the security verification approach;

b) Canada witnessing arrangements;

c) an outline of the security verification items; and

d) for each security verification item:

i) a description of the verification scenario;

ii) ordering dependencies; and

iii) expected results (i.e., pass/fail criteria).

(206) The Contractor must conduct security installation verification in accordance with the approved Security Installation Verification Plan for each of the test items in the security installation verification plan that includes:

a) the expected results (i.e., pass/fail criteria);

b) the actual results; and

c) a description of deviations and how each was resolved.

(207) The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

(208) The Contractor must implement patches and corrective measures as part of vulnerability assessment activity. Where this is not feasible (i.e., time to test patch or determine and test corrective measures

would seriously delay the project), the Contractor must create Problem Tickets for any required patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity.

(209) The Contractor must provide Canada with an updated SRTM that contains, for each security requirement to be tested by the Integration Security Test Plan, Vulnerability Assessment Plan and Security Installation Verification Plan, the tracing (a reference to an identifiable element) to integration security testing test cases.

5.5.2.3 SA&A In-Service

(210) The Contractor must receive Authority to Operate (ATO) to achieve the SA&A In-Service Ready Milestone.

5.5.3 Third Party Assessment

(211) The Contractor must complete a security assessment with an independent third party assurer, qualified under AICPA or CPA Canada and/or an ISO certification regime that conforms to ISO/IEC 17020 quality management system standards, at no additional cost to Canada that will prepare a Security Assessment Report that includes:

a) the legal business name of the Contractor;

b) current date and/or status of certifications and/or SOC 2 Type II report;

c) evidence to demonstrate compliance of the Service with Annex A-5 Security Requirements and other security requirements in the Contract;

d) name and address of the third party assurer that performed the security assessment; and

e) evidence that the third party assurer is qualified under AICPA or CPA Canada, and/or ISO certification regime that conforms to ISO/IEC 17020 quality management system standard.

(212) The Contractor and third party must provide additional data and responses to Canada's assessment of security risks and aid in mitigation of security risks within 5 FGWDs to aid in obtaining approval of the security assessment and authorization.

6 SERVICE LEVEL TARGETS (SLT)

(213) The Contractor must design, implement, manage and operate the Service Portal, Service Management and COAS Services to meet the Service Level Targets (SLTs) defined in this section.

(214) The Contractor acknowledges that all SLT's are based on key service performance metrics, which are measurable and must be constantly monitored by the Contractor, 7 days per week, 24 hours per day, 365 days per year, in order to accurately determine the on-going performance of all aspects of the COAS Service.

(215) The Contractor must commence Service Level Target and performance reporting for all COAS Service immediately in the Operations Phase and for the duration of the contract.

(216) The Contractor's COAS Service must meet or exceed the following specific monthly SLT's, excluding any agreed upon maintenance windows in the following Service Level Target Table: "

Service Level Target Table:

Service Level Target	Service Description
SLT-MTTR-COAS	Maximum Time to Restore the COAS, or any portion of the Service
SLT-MTTR-SP	Maximum Time to Restore the Service Portal
SLT-BA	Detailed Billing file accuracy, timing and format
SLT-OR	Operational Readiness

(217) The Contractor must make available the Service Level reporting information for COAS on the Contractor's Service Portal for access by the Technical Authority (or delegate), preferably no later than 10 FGWD's from the last day of the previous month.

(218) The Contractor must provide, at a minimum, individual data entries for each of the Service Level Target measurements specified in the Service Level Target Table including the raw data and the formula(s) used to calculate each result.

6.1 SLT-MTTR-COAS

(219) The Contractor acknowledges that the Service Level Target for MTTR failure must not exceed 2 hours for any Incident impacting COAS Services.

(220) The Contractor must add an SLT-MTTR-COAS failure to the Service Level Failure and Credit Report (SLFCR) for all COAS Service impacting Incidents that exceed 2 hours of outage time.

(221) The Contractor must measure MTTR on a per-Incident basis based on outage time of the Incident. Outage time is from the time the Contractor is aware of the outage until full restoration.

6.2 SLT-MTTR-SP

(222) The Contractor acknowledges that the Service Level Target for MTTR failure must not exceed 4 hours for any Incident impacting the Service Portal.

(223) The Contractor must add an SLT-MTTR-SP failure to the SLFCR for all Service Portal impacting Incidents that exceed 4 hours of outage time.

(224) The Contractor must measure MTTR on a per-Incident basis based on outage time of the Incident. Outage time is from the time the Contractor is aware of the outage until full restoration.

6.3 SLT-BA

(225) The Contractor acknowledges that the Billing Files (EBDF, SSC Summary Invoices and Client Summary Invoices) must by 100% accurate to meet the Service Level Target for Billing Accuracy. Accuracy of all file contents must include correct:

a) correct filename;

b) correct data and file contents (e.g., format, structure, data, etc.);

c) must comply to the electronic billing file format in Appendix 2 – Electronic Billing File to Annex A; and

d) monthly SSC and Client Summary Invoices must be compliant to the format as specified in the SRS and approved by the TA (or delegate).

(226) The Contractor must add an SLT-MTTR-SP failure to the SLFCR for any Incident that impacts billing files.

(227) The Contractor acknowledges, that to achieve the SLT, the Electronic Billing Detailed file and monthly summary invoice must be available for the calendar month within 10 FGWD's following the end of the previous month.

(228) The Contractor acknowledges, that to achieve the SLT, the Electronic Billing Detailed file and monthly summary invoice must comply to the electronic billing file format in Appendix 2 – Electronic Billing File to Annex A and the Monthly summary invoice and Client invoices must be compliant to the format identified in SRS Each instance of non-compliance (discrepancy) must be tracked as a separate SLT-BA failure.

6.4 SLT-OR

(229) The Contractor acknowledges that the Service Level Target for Operational Readiness (SLT-OR) is achieved by meeting all deliverable(s) and approval(s) as per Table entitled Project Milestones.

(230) The Contractor must add an SLT-OR failure to the SLFCR for all Project Milestones not met.

Shared Services Canada

Conferencing & Operator Assisted Service (COAS)

Annex B – Audio/Web Conferencing Statement of Work

Version 2.0

Table of Contents

1 Audio/Web Service (AWS)

(1) The Audio/Web Service (AWS) is a cloud based, self-serve on demand collaborative service and is accessible by either PSTN or internet connection using, but not limited to, a telephone, mobile device, computer, tablet from any location involving:

a) two (2) or more Participants speaking or collaborating with each other; or

b) A Webcast event which is streamed to a large audience.

(2) The AWS is comprised of three (3) conferencing types:

a) Self-Serve Audio Conference (SSAC);

b) Self-Serve Audio/Web Conference (SSAWC); and

c) Self-Serve Webcast Conference (SSWC).

(3) The Contractor must comply with the *Official Languages Act* which includes at a minimum:

a) that all aspects, including interfaces, chats, reports are presented in both of Canada's Official Languages (English and French) depending on the choice initiated by the Participant; and

b) that the Contractor's personnel are fluent in both of Canada's Official Languages (English and French).

(4) The AWS must allow a Subscriber to host an unlimited number of simultaneous SSAC, SSAWC and SSWC not to exceed a maximum per conference duration of 480 consecutive minutes (8 hours) from any country.

(5) The AWS, as implemented and managed by the Contractor, must meet or exceed all of the requirements listed in the Contract during the entire Contract period.

(6) The Contractor must provide all mandatory functions and features of the AWS, as described in Annex A – General SOW and Annex B – AWS SOW, in both of Canada's Official Languages. In addition, the Contractor must offer Canada all functions and features of the commercial AWS, for consideration by the Technical Authority (TA) (or delegate). The Contractor must make these available in Annex E –Financial Evaluation Worksheet for general ordering under this Contract no later than 10 FGWDs prior to the In-Service Date.

(7) Following Contract Award, the Contractor must also offer to Canada all functions and features, in both of Canada's Official Languages, that have been developed since Contract Award for consideration by the Technical Authority (TA) (or delegate). The TA will provide written acceptance of any features or functions that are selected for inclusion in the COAS Services. The Contractor must make these features and functions available in Annex E – Financial Evaluation Worksheet for ordering within 5 FGWDs of written acceptance by Canada throughout the remaining Contract Period.

(8) The Contractor must provide an audio conferencing service including all standard functions and features of a commercial conference offering, at a minimum, but not limited to:

a) telephone numbers (local and 1-800) for Audio Conference;

b) Audio Conference access code; and

c) Personal Identification Number (PIN) code.

1.1 Licensing

(9) The Active User Model, defined in the COAS contract describes an Active User as a Subscriber who accesses the audio/web application for a total minimum of 30 minutes of meeting activity per month for the months measured for calculation.

(10) The annual license fees will be based on the applicable Tier Pricing of the "Total Audio Web Annual License cost" multiplied by the number of Active Users either:

a) determined at contract award for Year 1; or

b) based on the methodology to calculate Active Users for each subsequent year of the contract.

(11) The number of Active Users for Year 1 of the contract will be determined by SSC at In-Service Date.

(12) The "methodology to calculate Active Users for each subsequent year of the contract" is the average of calendar months 8, 9 and 10 of each contract year. The "contract year" is defined as one (1) year starting on the anniversary of the In-Service Date.

Example Calculation of Active Users

Example anniversary In-Service Date = July 12th
Active User Count March = 9,500
Active User Count April = 11,500
Active User Count May = 6,000
Monthly Average User Count = (9,500 + 11,500 + 6,000)/3 = 9,000
Therefore, the number of Active Users = 9,000 for the purposes of calculating next year's annual license fees.

(13) Canada reserves the irrevocable right, yearly at each anniversary date, on an annual basis, to adjust, downwards or upwards, the amount of Active Users which may result in a change to the tier group.

1.2 Features and Functions

(14) The AWS must allow, at a minimum, the following features for all SSAC, SSAWC, and SSWC Conferences:

a) **Closed Captioning (English and French);** Closed captioning and subtitling are both processes of displaying text on a television, video screen, or other visual display to provide additional or interpretive information.

b) **Bridge Call Back functionality;** allows a meeting Participant to initiate a call from within the Web Conferencing Meeting application platform to connect audio for the Participant's connection.

c) **Call out functionality;** allows a Participant to initiate a call, and subsequently connect an additional Participant to the audio conference.

d) **Call in functionality;** ability for Participants to connect to the conference by dialling a telephone number.

e) **Audio Integration;** provide a flexible integrated audio that allows conference Participants to independently choose their audio preference, Public Switched Telephone (PSTN) or Voice over Internet Protocol (VoIP) and enables the same simultaneous experience for all Participants regardless of connectivity preference.

f) **Participant list;** A list of all connections to the conference, identifying each connection by the personal data obtained when the connection is established such as; Name, telephone number, email address.

g) **American Sign Language (ASL);** ASL is a complete and organized visual language that is expressed by both manual and nonmanual features.

h) **Simultaneous Interpretation (SI);** SI is when an interpreter translates the message from the source language to the target language in real-time.

i) **Recording;** Digital record of a Web Conference content and Participant interactions.

j) **Registration;** Ability for Participants to sign up for a conference in advance of the start date & time; providing the personal information requested by the conference Host or Co-Host and the ability for the Host or Co-Host to obtain information on who & how many Participants have signed up to attend the future conference.

k) **Whiteboard;** An interactive whiteboard is a display that reacts to input from a Participants or from other digital devices. It allows interactive real time sessions that include:

   i) viewing any action taking place while content is being edited and annotated by Participants;

   ii) dragging the pointer across the page and perform freehand drawing;

   iii) highlighting specific areas;

   iv) erasing content, inserting and modifying shapes (i.e., lines, arrows, squares, circles, etc.);

   v) undoing, redoing, copying, cutting and pasting content; and

   vi) saving the content of a whiteboarding session.

l) **Real time translation (RTT);** displays the Closed Captions in the alternate official language of Canada from the language being spoken. (ie., English -> French and French -> English).

m) **Share presentations;** the ability for Host and Participants to share materials, whether uploaded or open on the individual's device, for others in the conference to view, including files with an audio component to be shared within the conference.

n) **Notes;** a space within the conference where Participant(s) can take notes, meeting minutes, action items, etc. Notes can be saved and shared after the conference.

o) **Chat functionality;** send or a receive text messages to a selected Participant, or to all Participants simultaneously.

p) **Polling functionality;** provides real-time ability to record the opinion or vote of Participants

q) **Transcription**; a written record of all words spoken during a conference and can be downloaded and shared if needed.

r) **Webcasting functionality;** A webcast is a media presentation distributed over the Internet using streaming media technology to distribute a single content source to many listeners/viewers simultaneously.

s) **Streaming:** ability to continually transmit audio and video content from a server to viewers, via social media sites, (e.g., YouTube, Facebook).

t) **Video enabled;** A multi-point transmission of voice and video communication that allows multiple Participants to communicate in real-time where each Participant transmits a Unicast Stream and receives a combined Unicast Stream of other Participant's voice and video.

u) **Keyboard & mouse sharing control;** allows a Participant to move the cursor and type on a file being shared. The Participant that is sharing the file can regain control at any time.

v) **File sharing;** the ability for the Host to transfer files to Participants before, during, or after the conference.

w) **Post conference surveys;** displays a survey for Participants to complete after the conference ends either via a pop-up window or by redirecting the Participant to a website. Submitted survey results are available for the Host or Co-Host in the Host or Co-Host account's reports.

x) **Lobby**; A virtual environment where Participants to the conference can wait to be admitted by the Host or Co-Host of the meeting.

y) **Co-Host**; An individual can be permitted to assume the role and privileges of the meeting Host. It can be designated when scheduling the conference or during any live meeting.

z) **Breakout Sessions**; the ability to separate Participants into smaller groups within the meeting environment where they can collaborate, share ideas and move in or out of any session and/or return to the original meeting.

aa) **Q&A**; a feature that allows any conference Participant to post or reply to any question or comment made during the meeting. It can be directed at the entire conference or a specific individual.

bb) **Guest Speaker/Panelist roles**; a feature in any Web Conference that provides a unique invitation and privileges during the Web Conference. A panelist will be able to be seen and heard, view feedback, become a polling coordinator, manage polls and download or present files.

cc) **Virtual Labs;** a feature currently within the any session that allow Participants in various geographical locations with remote computers set up as a virtual lab to conduct tests or simulations.

dd) **In-conference testing and grading;** a feature currently in any session that allows Host or Co-Host to test and grade attendees on topis or concepts that have been introduced in your session. Allows Host or Co-Host to set the time limit, number of attempts and decide how the grade of the test is given.

ee) **Attention tracking/status**; a feature currently available in a Web Conference that allows Host or Co-Host to identify that Participants are engaged with the meeting. It provides indicators if an attendee has minimized the meeting window or brought another window in front of the meeting window and can generate a post meeting report with a summary of attentiveness.

ff) **Destination URL post conference;** Redirects Participants to a specific website (URL) after the conference ends. This may be to complete a survey and to direct Participants to additional information or resource materials.

gg) **Electronic Service Support;** a chat type functionality for end users to obtain in meeting assistance without requiring a telephone call.

1.3 Roles

1.3.1 Host / Co-Host

(15) The Web Conferencing Service must allow a Host or Co-Host to:

a) start and end a Web Conference;

b) remove a Participant from a Web Conference;

c) mute or un-mute selected Participant(s) or all Participant(s);
d) grant or remove Presenter status for a Participant;
e) disable/enable the video view for all Participants;
f) grant Host or Co-Host status to a Participant;
g) activate and de-activate all the features for Participants and Presenter;
h) lock and unlock access to the Web Conference to any new Participants;
i) view Participant's questions (chat);
j) provide an answer to any Participant's questions, either directly or by sharing the answer with all Participants.
k) conduct a poll with Participants with the results provided in real time;
l) display polling results to all Participants; and
m) save polling results to desktop.

(16) The Web Conferencing Service must allow the Host or Co-Host to:

a) create one or more Breakout Rooms, as required, each with its own private Audio Conference between Participants assigned to the Breakout Rooms;
b) observe individual sessions (Breakout Room), provide corrective input to Participants, move between sessions, or broadcast messages to Participant(s) across session boundaries;
c) distribute Participants to and from Breakout Rooms;
d) create and close Breakout Rooms;
e) participate in any Breakout Room;
f) post files for Participants to download to their desktops; and
g) return to original meeting.

(17) The Web Conferencing Service must include the ability for the Host or Co-Host or Participants to initiate and/or connect to a Web Conference from Microsoft Office 365 products.

1.3.2 Participants

(18) The Web Conferencing Service must allow a Participant to:

a) mute and un-mute their audio;
b) modify their Attention Indicator (active, non-active);
c) use all Host features when granted Host or Co-Host status;
d) use all Presenter features when granted Presenter status;
e) disable/enable video view from the Participant device;
f) transfer/regain control of their desktop (mouse and keyboard control) to/from the Host or Co-Host;
g) submit questions to the Presenter or Host or Co-Host (active or silent mode);
h) send one or more messages to a selected Participant or to all Participants;
i) share documents, applications, annotations, presentations and whiteboards with other Participants within a Breakout Room;

(19) The Web Conferencing Service must notify Participant(s) when the Web Conference has ended.

(20) The Web Conferencing Service must automatically share a presentation when a Participant joins a Web Conference.

(21) The Web Conferencing Service must allow a Participant to view a list of all Participants in the Web Conference that includes the Attention Indicator and the Participant that is actively speaking in the Web Conference.

1.3.3 Presenter

(22) The Web Conferencing Service must allow a Presenter to:

a) display one or more presentations to all Participants;
b) upload Presentations for viewing by all Participants;
c) view the list of Participant's questions;
d) answer any questions by answering the Participant who asked the question directly, or by sharing the answers with all Participants;
e) use all Participant features;
f) share viewing or control of a presentation with other Participant(s);
g) conduct a poll;
h) provide results of a poll to all Participants; and
i) save the results of a poll to the Presenter's device.

1.4 Audio Requirements

(23) The AWS must provide integrated audio conferencing (PSTN and computer audio (VoIP)) that allows Participants to communicate with other Participants (audio) in a Self-Serve Audio Conference (SSAC) Self-Serve Audio/Web Conference (SSAWC) and a Self-Serve Webcast/Webinar Conference (SSWC).

(24) The AWS must allow audio communications between other Participants that are using the SSAC, SSAWC, or SSWC service and support all features of the AWS as identified above in section 1.2 Features and Functions, in a SSAC, SSAWC, or SSWC.

(25) The AWS must, at a minimum, provide the following attributes:

a) A latency rate of 100 milliseconds (ms) or less;
b) Packet loss of <1% during any 15s interval;
c) Jitter <30ms during any 15s interval;
d) Noise cancellation between -20 and -30dB;
e) Clear, audible tones; and
f) Full-duplex communication.

(26) The AWS must, at a minimum, provide the following standards and protocols:

Protocols and Standards	Category					
	Media (Video)	Media (Audio)	Signaling	Encryption	Data	Control
RTP (transport)	X	X				
TCP	X	X				

UDP	X	X				
SRTP	X	X		X		
H.264 AVC (compression)	X					
H.264 SVC (compression)	X					
H.265 HEVC (compression)	x					
SILK (Opus, compression)		X				
G.711 (compression)		X				
G.722 (compression)		X				
G.722.1 (compression)		X				
G.723.1 (compression)		X				
G.728 (compression)		X				
G.729 (compression)		X				
AAC-LC (compression)		X				
AAC-LD (compression)		X				
LPCM		X				
SIP (IP)			X			
SIPS (IP)			X			
H.323 (IP)			X			
H.320 (ISDN)			X			
TIP			X			
WebRTC			X			
TLS (for SIP)			X	X		
Q.931 (for H.323,ISDN)			X			X
H.235 (for H.323)				X		
H.239 (data)					X	
T.120 (data)					X	
H.221 (for H.320)						X
H.225 (for H.323)						X
H.231 (for H.320)						X
H.242 (for H.320)						X
H.243 (for H.320)						X
H.245 (for H.323)						X

H.460 (Firewall traversal for H.323)						X
ICE/TURN & STUN (Firewall traversal for SIP)						X

1.4.1 Dual Tone Multi-Frequency Commands

(27) The AWS must allow the Host or Co-Host to be given control of the SSAC, SSAWC, or SSWC with Dual Tone Multi-Frequency (DTMF) invoked commands involving two or fewer keystrokes (not involving switch-hook flash) to:

a) confer privately with the Service Desk without disconnecting from the SSAC, SSAWC, or SSWC;

b) request the Service Desk to join the Audio Conference;

c) Lock or Unlock access to Participants (only the Host or Co-Host);

d) confer privately with any Participant without disconnecting the SSAC, SSAWC or SSWC Conference (e.g., sub-conferencing) (only the Host or Co-Host);

e) disable the entry or exit DTMF tones;

f) start/stop the SSAC, SSAWC or SSWC Conference Recording (only the Host or Co-Host);

g) place all Participants into “listen only” mode (only the Host or Co-Host);

h) mute or un-mute the Host or Co-Host;

i) hear a count of the number of Participants;

j) hear a list of available DTMF keypad commands;

k) hear a list of Participants names if captured on entry to the conference and feature has been enabled;

l) terminate the SSAC, SSAWC or SSWC Conference (only the Host or Co-Host);

m) Dial Out to Participant(s) and subsequent DTMF commands to rejoin the SSAC, SSAWC or SSWC with or without new Participant(s) or to connect new Participant to a SSAC, SSAWC or SSWC Conference & continue dialing out to additional Participant(s) (only the Host or Co-Host).

(28) The AWS must allow Participants to invoke DTMF commands involving two or fewer keystrokes (not involving switch-hook flash) to:

a) privately confer with the Service Desk without disconnecting from the SSAC, SSAWC or SSWC;

b) mute or un-mute;

c) hear a list of available keypad DTMF commands; and

d) hear a count of the number of Participants.

1.5 AWS Peak Capacity

(29) The Self-Serve Audio Conference (SSAC) must allow the following, at a minimum;

a) 500 Participants for a single Self-Serve Audio Conference from any country;

b) 5000 Participants in all concurrent SSACs;

c) 2500 concurrent SSACs;

d) an maximum duration per SSAC, not to exceed 480 consecutive minutes (8 hours), where Participants are inactive; and

e) maximum of 60 minutes (1 hour) per SSAC if the 2 or fewer Participants.

(30) The Self-Serve Audio/Web Conference (SSAWC) must allow the following, at a minimum;

a) 3000 Participants for a single SSAWC from any country;

b) 5000 Participants in all concurrent SSAWC; and

c) 20,000 concurrent SSAWC Conferences.

(31) The Self-Serve Webcast Conference (SSWC) must allow the following, at a minimum:

a) 3000 Participants for a single SSWC from any country;

b) 5000 Participants in all concurrent SSWC;

c) 20,000 concurrent SSWC Conferences; and

d) the streaming to a minimum of 10,000 Participants.

1.6 Conference Recordings

(32) The AWS must allow an SSAC, SSAWC or SSWC Recording for each of the AWS of unlimited duration.

(33) The Contractor must not modify an SSAC, SSAWC, or SSWC Conference Recording unless authorized by the Technical Authority (TA) (or delegate).

(34) An SSAC Conference Recording must be automatically available for download from the Service Portal within a maximum of 60 minutes from the end of an SSAC in formats specified by the Technical Authority (or delegate) at Contract Award.

(35) The SSAWC Conference Recording and the SSWC Recording must be automatically available for download from the Service Portal within 120 minutes from the end of a SSAWC or SSWC in formats specified by the Technical Authority (or delegate) at contract award.

(36) The AWS must automatically send an email to the Host within 15 minutes of the completion of an SSAC, SSAWC, or SSWC Conference Recording with instructions on how to download the SSAC, SSAWC, or SSWC Conference Recording with notification that the recording will only be available for 30 days from date of creation.

(37) The Contractor must automatically delete an SSAC, SSAWC, or SSWC Conference Recordings 30 days after the end date of the conference.

1.7 Software Requirements

(38) The AWS must be available to all Participants without requiring a software application to be installed on any of the following devices:

i) Desktop;

ii) Laptop;

iii) Tablet device; and

iv) Mobile device.

(39) The Contractor must ensure that any software (such as plug-ins, add ins, applets), barring security limitation imposed by GC systems, that are necessary for devices to use the COAS Services:

i) are downloaded or available for download, installed and configured without requiring any actions other than responding to dialog boxes;

ii) does not require the use of Adobe Flash or third party software; and

iii) can be used without requiring the participant to have device administrative rights.

(40) The AWS must fully operate (all features) with, at a minimum, the following internet browsers including new browsers as they become available, on devices connecting to the Service:

i) Chrome 70 or later;

ii) Safari 12.0 or later;

iii) Firefox 65 or later;

iv) IE 11 or later; and

v) Edge 18 or later.

2 Self-Serve Audio and/or Web Conference and Webcast

(41) The Contractor's Audio/Web Application platform must allow a Subscriber to schedule any of the following conference types, which may or may not require Participant registration.

a) Audio only conference (SSAC);

b) Audio/Web conference (SSAWC); and

c) Webcast and Webinars (SSWC).

2.1 Scheduling a Self-Serve Audio and/or Web Conference (SSAC and SSAWC)

(42) The Contractor's Audio/Web Application platform must allow a Subscriber to schedule an SSAC or SSAWC using a web-based tool and Outlook extension that includes the functionality to:

a) schedule a single or recurring instance of an SSAC, SSAWC and SSWC in the Outlook Calendar, if applicable, up to 1 year in advance of the date of the audio or web conference that includes:

i) selecting the start date and time of the audio and/or web conference;

ii) selecting the duration of the audio and/or web conference;

iii) selecting the frequency of the audio and/or web conference (I.e., daily, weekly, monthly, multiple instances successively);

iv) entering the email addresses of the Participants (optional);

v) selecting email addresses of Participants from Microsoft Outlook Contacts and/or address book (if applicable);

vi) entering an agenda (optional);

vii) entering a welcome message (optional);

viii) entering audio or web conference features to be enabled or disabled (e.g. Participant features, Presenter features, chat, etc.); and

ix) scheduling simultaneous interpretation meetings and assigning interpreters.

b) Modify or cancel a scheduled audio and/or web conference;

(43) The Contractor's Audio/Web Application platform must automatically send an email to the Subscriber and all invited Participants in both Official Languages (English and French) of the conference details that includes:

a) time and date of the audio and/or web conference;

b) duration of the audio and/or web conference;

c) audio conference telephone numbers (if applicable);

d) Host name and telephone number;

e) Toll free number of the Contractor's Service Desk;

f) password to access the audio and/or web conference (if applicable); and

g) URL of the scheduled web conference.

(44) For all modifications or cancellations of scheduled audio and/or web conference, the Contractor's Audio/Web Application platform must automatically send an email to all Participants, in both Official Languages (English and French) from Outlook Calendar, if applicable, with notification of the conference modification or cancellation.

2.2 Scheduling a Self-Service Webcast Conference (SSWC)

(45) The Contractor's Audio/Web Application platform must allow a Subscriber to schedule a SSWC event using a web-based tool and Outlook extension that includes the capabilities to:

a) schedule a single or recurring instance of an SSWC in Outlook Calendar (optional) that includes:
   i) selecting the start date and time of the SSWC;
   ii) selecting the duration of the SSWC;
   iii) selecting the frequency of the SSWC (daily, weekly, monthly, multiple instances successively);
   iv) entering the email addresses of the Participants (optional);
   v) selecting email addresses of Participants from Microsoft Outlook Contacts and/or address book (if applicable);
   vi) entering an agenda (optional);
   vii) enter names of guest speakers or Presenters;
   viii) entering a welcome message (optional); and
   ix) entering SSWC features to be enabled or disabled, including but not limited to Presenter features, chat, polling.

(46) The Contractor's Audio/Web Application platform automatically sends an email to the Subscriber and all invited Participants in both Official Languages (English and French) of the SSWC details that includes:

a) time and date of the SSWC;
b) duration of the SSWC;
c) Host name and guest speaker names;
d) Toll free number of the Contractor's Service Desk;
e) password to access the SSWC (if applicable); and
f) URL of the scheduled SSWC.

2.3 Participant Registration

(47) The Contractor's Audio/Web Application platform must allow a Subscriber to choose the registration feature to register for the SSAC, SSAWC or SSWC using a web-based tool and Outlook extension that includes:

a) request Participants to register for an SSAC, SSAWC or SSWC that includes:
   i) entering the email addresses of the Participants that will be invited to register for the SSAC, SSAWC or SSWC (optional);
   ii) selecting email addresses or Participants from Microsoft Outlook Contacts and address book (optional);
   iii) entering the maximum number of Participants that can register for the SSAC, SSAWC or SSWC;
   iv) identifying if approval is required for Participants registering for the SSAC, SSAWC or SSWC (yes or no);
   v) entering the registration password (optional);
   vi) requesting registration id (optional);

vii) selecting registration questions (e.g., first name, last name, telephone number, address, company etc.) based on data entry method (e.g., text box, check box, option buttons, drop down list), allowable data entry content and data entry status (e.g., optional, mandatory); and

viii) allow the Host or Co-Host to review the registered Participants for the SSAC, SSAWC or SSWC.

ix) automatically sends an email to approved Participants following completion of the registration request in both Official Languages (English and French) that include:

a. Host, and guest speaker (if applicable) names;

b. Name of a SSAC, SSAWC or SSWC;

c. duration of the SSAC, SSAWC or SSWC;

d. Toll free number of the Contractor's Service Desk; and

e. URL of the SSAC, SSAWC or SSWC.

(48) The Contractor's Audio/Web Application platform must automatically send an email for the SSAC, SSAWC or SSWC registration in both Official Languages (English and French) to Participants that have registered for the SSAC, SSAWC or SSWC where approval is not required.

3 Self-Serve Audio Conference (SSAC)

(49) The AWS must allow Subscribers to initiate or schedule an SSAC including all of the following functions:

a) Initiate an ad hoc conference:
   i. Invite conference Participants;
   ii. Add new Participants during in-session; and
   iii. Select additional service features, if required.

b) Schedule a conference:
   i. Schedule a conference type from the audio/web conferencing application platform;
   ii. Select date and time; and
   iii. Select additional service features, if required.

c) Change a conference:
   i. Changing date and time;
   ii. Change service features, if required;
   iii. If changing conference type:
      1. Cancel original scheduled conference; and
      2. Reschedule with the required conference type.

d) Cancel conference:
   i. Send email to Participants with cancellation notification.

(50) Contractor must send an email to Subscriber with the following information;
   i. telephone numbers (local and 1-800) for SSAC;
   ii. SSAC access code;
   iii. PIN Code.

(51) The Contractor must provide, on demand SSAC inclusive of, but not limited to, the following features:

a) allow a Subscriber to initiate or schedule an SSAC using the conferencing platform feature;

b) conduct an SSAC in accordance with the initiation or scheduling request associated with the SSAC;

c) allow the Subscriber to add a customizable secondary SSAC access code that must be keyed-in by Participants, in addition to the primary SSAC access code, to access the SSAC;

d) provide the capability within the Outlook client to allow SSAC connection information to be inserted into a conference invitation;

e) allow any Participant, who is unable to access an SSAC, to obtain real-time assistance from the Service Desk using a Dual Tone Multi-Frequency (DTMF) invoked by *0* or any other star touch (*) command;

f) direct a Participant to the Service Desk, on the third (failed) attempt to access an ASSAC;

g) ensure that the language of preference (English or French) selected by the Participant when entering the SSAC is used for the prompts and recordings;

h) terminate an SSAC when all Participants have disconnected from the SSAC or after 480 consecutive minutes (8 hours) if one only one Participant remains connected;

i) full-duplex communication;

j) functionality to accept both incoming Public Switched Telephone Network (PSTN) connections and computer audio connections;

k) provide the following announcements for a SSAC using digitized voice or system tones developed in consultation with the Technical Authority (or delegate) for each announcement:

i) a disclaimer announcing to all Participants that these conferences are not to be used for classified or protected discussions;

ii) to Host or Co-Host and Participants and/or Operator when joining or exiting a SSAC;

iii) to Host or Co-Host and the Participants prior to being answered by the Service Desk;

iv) to Participants upon activation/deactivation of SSAC Conference Recording including those who subsequently join the SSAC with an active SSAC Conference Recording;

v) if the Service Desk has been requested or request cancelled by the Participant;

vi) if Locked Access has been enabled or disabled;

vii) to Participants when entering or exiting the question and answer queue;

viii) for step-by-step procedures to allow the Host to access a SSAC;

ix) for step-by-step procedures to allow Participants to access a SSAC;

x) for list of available features and their associated keypad commands for the SSAC;

xi) to mute/unmute by Host or Co-Host or Participant; and

xii) for list of recorded names of Participants (if roll call was activated before accessing the SSAC) in the SSAC.

4 Self-Serve Web Conference and Webcast (SSWC)

(52) The SSWC, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in the Contract for during the entire Contract period.

(53) In addition to the requirements identified in this section, the SSWC must provide all functions and features of the commercial offering of web conferencing services provided by the Contractor to other clients of the Contractor.

(54) The SSWC must schedule and allow a Web Conference in accordance with the Web Conference Reservation associated with the Web Conference.

(55) The Contractor must implement and manage a Web Conference Service allowing Subscribers and Participants to collaborate in conducting business meetings and seminars, lead presentations, provide online education and offer support via remote keyboard mouse control.

(56) The Contractor must provide, on demand SSWC inclusive of, but not limited to, the following features:

a) allow a Subscriber to initiate or schedule an SSWC using the conferencing platform feature;

b) allow the Subscriber or any Participant to commence a web session;

c) allow a Host to transfer control of the session among Participants, so any Participant can act as the Host or co-Host;

d) conduct a SSWC in accordance with the initiation or scheduling request associated with the SSWC;

e) provide the capability within the Outlook client to allow SSWC connection information to be inserted into a meeting invitation;

f) ensure that the language of preference (English or French) selected by the Participant when entering the SSWC is used for any prompts and recordings;

g) terminate an SSWC when all Participants have disconnected or after 480 consecutive minutes (8 hours) if one only one Participant remains connected;

h) full-duplex communication;

i) functionality to accept both incoming PSTN and VoIP connections;

j) must provide chat support functionality for Participants requiring support during an SSWC; and

k) functionality for the Host or Co-Host to view the following information for an SSWC and action an issue if required (e.g., mute/unmute):

i) current and historical data associated with a scheduled SSWC including records of all changes;

ii) Host name;

iii) number of Participants;

iv) Participant actively speaking;

v) status of entry notifications (enabled, disabled);

vi) status of exit notifications (enabled, disabled);

vii) status of mute for each Participant (enabled, disabled);

viii) status of Locked Access (enabled, disabled);

ix) length of time that a Participant has waited in queue for a Service Desk, either to join the SSWC or for assistance;

x) number of Participants in the SSSWC; and

xi) status of SSWC Conference Recording (activated, deactivated).

Shared Services Canada

Conferencing & Operator Assisted Service (COAS)

Annex C – Operator Assisted Service Statement of Work

Version 1.1

Table of Contents

1 Operator Assisted Service (OAS)

(1) The Operator Assisted Services (OAS) is an Operator managed audio conferencing service that must be designed for scalable and robust capacity, including the automatic invocation by Canada to accommodate emergency events as specified in section 2 of Annex C – OAS SOW.

(2) The Contractor's Operator initiates the audio conference and assists the Participants in the placement of an audio connection, either through live or automated intervention, as required.

(3) In an unbiased and consistent manner, the Contractor must handle the following activities:

a) How conferences are fairly and equitably rescheduled as a result of scheduling conflicts; and

b) How Participants are queued for in-conference Questions & Answers (Q&As).

(4) The Contractor must ensure that their Operators are fluent (i.e., written, spoken and reading comprehension) in both of Canada's Official Languages (English and French) and perform the following activities for the application platform deployed:

a) Support the complete feature set and functionality of OAS found in Section 1.4 below.

b) Support the use of the application platforms that adheres to the Accessibility, Accommodation and Adaptive Computer Technology program (AAACT)[1], involving considerations such as:

i. protocols and procedures that allow Participants with disabilities to communicate with other Participants, including designated speaking opportunities and giving them the option to signal that they would like to speak, using American Sign Language (ASL) as a minimum;

ii. accommodating telecommunications devices such as teletype devices (TTY);

iii. Closed captioning; and

iv. ensure best-effort compatibility with universally approved accessibility input devices available to Participants with disabilities attending web and video conferences.

(5) The Contractor must provide an OAS, as and when scheduled, via a Service Portal. The OAS must allow for a scalable number of simultaneous conferences as defined in the Section entitled "Capacity" and number of participants serving Canadian interests both domestically and internationally for each conference type, when requested.

(6) The Contractor must provide, at a minimum the following OAS conference types:

Conference Type	Description
1. Press Conferences (PC)	• May involve a panel of speakers who provide updates and address questions from the media organizations remotely • Highly standardized • Focus is on the Questions & Answers (Q&A) • Important to know who is asking the questions & how to prioritize
2. Virtual Events (VE)	• Large gatherings that include Simultaneous

[1] Accessibility, Accommodation and Adaptive Computer Technology (AAACT) - Canada.ca

	Interpretation (SI), such as: • Award ceremonies • Program launches • Major initiatives • Annual meetings
3. Briefings/feedback to Large Groups (BRIEF)	• Is an interactive forum where all participants participate equally. • Can be interpreted or not —either English-only, French-only, or both French and English.
4. Collaborative Conferences (CC)	• Collaborative discussions and decision-making among senior leadership, often not requiring the Operator for monitoring the full conference duration.
5. Emergency Conference (EC)	• As described in section 2 of Annex C.
6. Custom Conferences (CUSTOM)	• Does not fit into any of the above categories

(7) The Contractor must deliver OAS by deploying either:

i) Operators that are Contractor resources;

ii) Operator assisted functionalities of a conferencing platform; or

iii) A combination of above.

(8) The following are examples of features and functionality that may be platform dependent and must be available within the timelines following the conference, as outlined in the Reporting Section in Annex A, Section 3.3:

a) Final registration;

b) Participant List;

c) Chat;

d) Q&A results; and

e) Conference recording

(9) The OAS must be delivered by an Operator and the service can be supported by the automated functionality of an application platform.

(10) The Contractor must offer to Canada, at no additional cost, any new features and service enhancements including those which are not yet part of the OAS (including service offerings made to other clients of the Contractor) as they become available and/or standard.

1.1 Languages of Service (English and French)

(11) The Contractor must provide Operators who communicate (i.e., speak, read, write) fluently in both of Canada's Official Languages without the need for a translator, to speak in the language selected by the Participant (English or French). The Contractor must provide the same user experience regardless of whether a Participant chooses English or French.

1.2 Security Clearance Requirement

(12) The Contractor's Operators must meet the Security Clearance Levels identified in the Security Requirements Checklist (SRCL).

1.3 Professional Skill Requirement

(13) The Contractor's Operators will be required, as a minimum, to interact with the following types of Participants: members of the media, the GC, provincial and municipal government personnel up to and including key senior government and private corporation officials. As such, the Operators must have the training, experience, and professionalism to effectively deliver a professional and courteous OAS Participant experience.

1.4 OAS Attributes and Features

(14) The OAS must, at a minimum, provide the following attributes:

a) No latency in voice;

b) Noise cancellation;

c) Clear, audible tones; and

d) Full-duplex communication.

(15) The OAS must allow, at a minimum, for the following features:

a) **Closed Captioning (English and French);** Closed captioning and subtitling are both processes of displaying text on a television, video screen, or other visual display to provide additional or interpretive information.

b) **Bridge Call-back functionality;** allows a Participant to connect audio by initiating a call from within the audio conference.

c) **Operator Call-out functionality;** allows the Operator to initiate a call to a Participant and subsequently connect that Participant to the audio conference.

d) **Call-in functionality;** allows Participants to connect to the audio conference by dialling a telephone number.

e) **Audio Integration;** provide a flexible integrated audio that allows conference Participants to independently choose their audio preference - Public Switched Telephone (PSTN) or Voice over Internet Protocol (VoIP).

f) **Mobile Integration;** complete collaboration and integration for Participants using virtually any device, including Android, iOS, as well as across desktop platforms (PC or Mac) to participate in audio calls and/or video conferencing.

g) **Participant list;** a list of all Participants connected to the audio conference, identifying each connection by the personal data obtained when the connection is established (e.g., name, telephone number, email address).

h) **Recording capabilities:** Digital record of an audio conference content including Participant interactions.

i) **Q&A;** a feature that allows any conference Participant to post or reply to any question or comment made during the meeting. It can be directed at the entire conference or a specific individual.

j) **Participant registration capabilities;** allows Participants to sign up for a conference in advance of the start date and time by providing the information requested by the conference Host or Co-Host and allows the Host or Co-Host to obtain details of the number and identity of registered conference Participants.

k) **Communication Line;** allows an Operator to facilitate a private conversation with an authorized person not participating in the conference for the purpose of managing the conference using an audio call or private audio conference.

l) **Conference Web App for Host or Co-Host;** web page or web-based application that allows a Host or Co-Host to do all the following, at a minimum: view Participants connected to the conference, view Participants that have been queued for questions, manage Q&A priorities, and chat with the Operator.

m) **Electronic Service Support;** a chat type functionality that allows Participants to obtain live assistance during the conference without requiring a telephone call.

1.5 Operator Responsibilities

(16) The Contractor's Operators must, at minimum, provide the following service features, when requested by a Subscriber:

a) A 30 minute pre-conference consultation with Subscriber, so that conference objectives, agenda, and roles and responsibilities (including backup plan) are understood;
b) Dry-run or rehearsal;
c) Recording;
d) Test lines set up for interpretation, if required;
e) Call-out Feature (ability for Operator to add Participants when they are having issues or other reasons);
f) Transcribing the names of Participants joining by PSTN;
g) Pre-authorized Participants list and/or additional password;
h) 30 minute pre-conference start, to conduct quality tests; and
i) An Operator with the following responsibilities:
    i) Meeting starts on time;
    ii) Enable and disable entry and exit notifications;
    iii) Enable and disable audio conference recording;
    iv) Must conduct a roll call, if requested;
    v) Ensures interpreters, Presenters, key panel Participants have joined successfully
    vi) Activation of requested features (recording, mute all Participants except Presenter, etc.);
    vii) Plays music on-hold while Participants wait;
    viii) Reads script to welcome and address administrative considerations;
    ix) Passes to meeting Host or Co-Host to do introductions and begin meeting; and
    x) Actively listens during meeting to:
        1. Answer any technical questions from attendees and Presenters;
        2. Run polls, manages chat, Q&A (Using standard script), and monitor audio quality; and
        3. Mute or un-mute as required.

2 Emergency Conferences and Emergency Events

(17) The Contractor's OAS must be designed with robust capacity to ensure scalability for emergency conference(s) and emergency event(s), as further defined below.

2.1 Emergency Conferences

(18) Emergency Conference is any conference required to be held with less than 2 hours' notice.

(19) The Contractor must provide the TA (or delegate) an automated written notification (in English and in French) immediately upon Canada's request for an Emergency Conference.

(20) There are two types of Emergency Conferences that may be requested and may involve Emergency Events:

Emergency Conference Classification	Length of Advance Notice
Emergency Conference Type 1	30 minutes or less
Emergency Conference Type 2	Greater than 30 minutes but less than 120 minutes (2 hours)

2.2 Emergency Events

(21) An Emergency Event is an occurrence of a domestic or global emergency, as determined in SSC's sole discretion, that will require a sharp increase in demand of OAS usage. Each Emergency Event commences upon notification by SSC to the Contractor and will persist until SSC informs the Contractor the Emergency Event is over.

(22) An Emergency Event will trigger an Emergency Conference.

(23) Upon notification by SSC of an Emergency Event, the Contractor must immediately meet with the Contracting Authority and Technical Authority (or delegates) to establish emergency measures, timelines and appropriate scaling of the OAS to respond to the Emergency Event.

(24) The Contractor must provide flexibility in the number of resource(s) required to address the Emergency Event.

(25) The rates identified in Annex E – Financial Evaluation Worksheet will apply for the duration of the Emergency Event.

3 OAS Scheduling

3.1 Managing Conference Requirements

(26) The OAS must allow a Subscriber to:

a) Create a conference up to 1 year in advance of the conference date for a single or recurring instance that includes the following and that is confirmed by email to the Subscriber within 15 minutes of creation:

i) select the conference type;

ii) select the date, time and duration of the conference including recurring conferences;

iii) modify the date, time and duration of the conference including recurring conferences;

iv) select the frequency of conferences including recurring conferences (I.e., daily, weekly, monthly, multiple instances successively);

v) include the contact information for the Subscriber (I.e., email address and phone number);

vi) enter the subject of the conference;

vii) enter the names of guest speakers;

viii) enter the names and phone number of Participants for Dial-Out conferences to be called by the Operator (if required);

ix) select conference features specified in section 1.4 of Annex C – OAS SOW to be enabled or disabled;

x) enter the maximum number of reserved ports required for Participants;

xi) modify the number of reserved ports up to 30 minutes before a conference; and

xii) Provide Participant prompts that indicate what information must be entered by a Participant prior to joining the conference.

b) Modify any aspect of an existing conference; a confirmation email must be sent by the Contractor to a Subscriber within 15 minutes of the modification; and

c) Cancel an existing conference; a confirmation email must be sent by the Contractor to the Subscriber within 15 minutes of cancellation.

(27) The OAS must automatically send an email to a Subscriber in the language of their choice (English or French) that includes:

a) Meeting details;

b) Time, date and duration of the conference;

c) Subscriber contact information;

d) Participant name and dial-out telephone numbers (if applicable);

e) Type of conference

f) Associated conference telephone numbers (local, toll free);

g) Access code;

h) Toll free number of the Contractor's Service Desk;

i) the URL and password to access a web application for the Subscriber to view the conference Participants, questions queued for the Host or Co-Host, chat window for the Operator(s) etc., if applicable;

j) Ongoing updates to the Participant registration lists, if applicable, must be available to the Host or Co-Host.

k) The rescheduling and cancellation policy that includes the following chargeable fees:

i. unused port(s) (a reserved port with no usage);
ii. cancellation in less than 24 hours' notice;
iii. Emergency Conference Type 1 (scheduled < 30 minutes before start); and
iv. Emergency Conference Type 2 (scheduled >30 minutes but less than 120 minutes)
v. Rescheduling policy and fees; and

l) Other comments, as approved by Canada.

(28) The Contractor must escalate any scheduling conflict that cannot be resolved in 60 minutes to the Technical Authority (or delegate).

3.1.1 Scheduled Operator Assisted Conference

(29) The Operator, if requested, must provide a Call-Out service to identified Participants specified in the Operator Assisted Conference Schedule no earlier than 10 minutes prior to the start of the Audio Conference.

(30) The OAS must allow a Participant to call the telephone number specified in the Audio Conference Schedule whereby the:

a) call is answered by the Operator (Dial-in to Operator) who adds the Participant to the Operator Assisted Conference and the Participant verbally provides a conference access code, reference information (e.g., reservation number for the Operator Assisted Conference, title of the Conference, name of Presenter) or Host or Co-Hosts name; and/or

b) Participant enters an Audio Conference access code to identify the Audio Conference they want to join.

(31) The OAS must allow the Host or Co-Host in a Scheduled Operator Assisted Conference to use either a web browser or have a private conversation with the Operator to:

a) view names of all Participants;

b) view names of Participants that have queued questions;

c) change the order of the questioners queued; and

d) have a private conversation (e.g., chat) with the Operator.

(32) The OAS must allow a private conversation between an Operator and an authorized person not participating in the Conference by using an audio call and/or chat session accessed with a public URL and authentication process approved by Canada (e.g., reservation number and passcode).

(33) The Operator must conduct a question and answer session, if required, for an Operator Assisted Conference by allowing Participants to indicate they have a question or join a queue of Participants who wish to ask a question using the keypad on their telephone, which the Operator puts in a "queue" of questions to be submitted to the Host (or Co-Host).

3.2 Dual Tone Multi-Frequency Commands

(34) The OAS must allow the Host or Co-Host to be given control of the conference with Dual Tone Multi-Frequency (DTMF) invoked commands involving three or fewer keystrokes (not involving switch-hook flash) to:

a) confer privately with the Operator without disconnecting from the conference;
b) request the Operator to join the conference;
c) lock or unlock access to Participants;
d) confer privately with any Participant without disconnecting from the conference (e.g., sub-conferencing);
e) disable the entry or exit DTMF tones;
f) start/stop conference recording;
g) place all Participants into "listen only" mode;
h) mute or un-mute the Host or Co-Host;
i) hear a count of the number of Participants;
j) hear a list of available DTMF keypad commands;
k) hear a list of Participant names if name recording has been enabled on entry to the conference;
l) terminate the conference; and
m) Dial Out to Participant(s) and subsequent DTMF commands to rejoin the conference with or without any new Participant(s) or to connect any new Participant to the Conference & continue dialing out to additional Participant(s) (only the Operator).

(35) The OAS must allow Participants to invoke DTMF commands involving three or fewer keystrokes (not involving switch-hook flash) to:

a) privately confer with the Operator without disconnecting from the conference;
b) mute or un-mute the Participant;
c) hear a list of available keypad DTMF commands;
d) hear a count of the number of Participants; and
e) enter/exit the question and answer queue.

3.3 OAS Peak Capacity

(36) The Contractor must have the capacity to provide the OAS with the following requirements, at a minimum:

a) up to 350,000 total conference minutes per month;
    i) conferences must support 1000 ports per conference;
    ii) support for 250 conferences per month; and
    iii) support for 10 simultaneous conferences.

(37) The Contractor must provide the Technical Authority with calculations used to determine scaling and capacity requirements for Emergency Event planning within 20 FGWDs of Contract Award.

4 Operator Assisted Conference Recordings

(38) The OAS must allow for the Host or Co-Host to choose a conference recording for any Operator Assisted Conference, inclusive of Breakout Rooms, regardless of duration.

(39) The Contractor must provide recordings in all of Canada's Official Languages (English and French) spoken during the conference (e.g., one for floor audio, one for English and one for French).

(40) The Contractor must not modify a conference recording.

(41) A conference recording must be automatically available for download within 60 minutes of the end of a conference in MP3 or MP4 format.

(42) The OAS must automatically send an email to the Host or Co-Host within 15 minutes of the completion of the conference with instructions on how to download the conference recording.

(43) The OAS must automatically delete a conference recording no sooner than 30 days after the end date of the conference.

(44) The OAS must allow a Subscriber with a Service Portal Account to manage conference recordings using a web-based application that includes the following features:

a) searching for conference recordings by selected filters including all of the following: scheduled date, scheduled time, meeting subject, meeting title, Subscriber name, and meeting identifier;

b) downloading the selected conference recording(s) in MP3 or MP4 format as selected by the Subscriber; and

c) deleting one or more conference recordings selected from a search where the Subscriber is requested to confirm the deletion request before deleting the conference recording(s).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
P2P 105809
Security Classification / Classification de sécurité Unclassified

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

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

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

4. Brief Description of Work / Brève description du travail

This SRCL is for an RFP that will be used to eventually have a "Conferencing & Operator Assisted Services" (COAS) contract in place.
The COAS will provide a modern Audio and Web conferencing platform solution which will also be used for the provision of the Operator Assisted Services.
Once in place, this contract will replace the Government Teleconferencing Services (GTS) contract as well as the Canada Conferencing Services (CCS).

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	☒ No / Non	☐ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	☒ No / Non	☐ Yes / Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☒ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☒ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit?	☒ No / Non	☐ Yes / Oui

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

Canada ☒	**NATO / OTAN** ☐	**Foreign / Étranger** ☐
7. b) Release restrictions / Restrictions relatives à la diffusion		
No release restrictions Aucune restriction relative à la diffusion ☒ Not releasable À ne pas diffuser ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	All NATO countries Tous les pays de l'OTAN ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :	No release restrictions Aucune restriction relative à la diffusion ☐ Restricted to: / Limité à : ☐ Specify country(ies): / Préciser le(s) pays :

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

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

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

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

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

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

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

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

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

Special comments:
Commentaires spéciaux : Additional clearances or verifications may be required by certain departments (To be confirmed).

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

10. b) May unscreened personnel be used for portions of the work? — ☒ No / Non ☐ Yes / Oui
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

If Yes, will unscreened personnel be escorted? — ☐ No / Non ☐ Yes / Oui
Dans l'affirmative, le personnel en question sera-t-il escorté?

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

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

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

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

PRODUCTION

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

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

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

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

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

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

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

SUMMARY CHART / TABLEAU RÉCAPITULATIF

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

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

☒ No / Non ☐ Yes / Oui

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

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

☒ No / Non ☐ Yes / Oui

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

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
P2P 105809
Security Classification / Classification de sécurité Unclassified

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

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

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Charbel El-Helou	Director, Conferencing Services	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
613-898-2723		charbel.el-helou@ssc-spc.gc.ca	2022-01-19

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

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

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

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

16. Procurement Officer / Agent d'approvisionnement

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

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

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

Stephanie Tompkins

Contract Security Officer

Stephanie.tompkins@tpgsc-pwgsc.gc.ca

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

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

Instructions for completion of a Security Requirements Check List (SRCL)

The instruction sheet should remain attached until Block #17 has been completed.

GENERAL - PROCESSING THIS FORM

The project authority shall arrange to complete this form.

The organization security officer shall review and approve the security requirements identified in the form, in cooperation with the project authority.

The contracting security authority is the organization responsible for ensuring that the suppliers are compliant with the security requirements identified in the SRCL.

All requisitions and subsequent tender / contractual documents including subcontracts that contain PROTECTED and/or CLASSIFIED requirements must be accompanied by a completed SRCL.

It is important to identify the level of PROTECTED information or assets as Level "A," "B" or "C," when applicable; however, certain types of information may only be identified as "PROTECTED". No information pertaining to a PROTECTED and/or CLASSIFIED government contract may be released by suppliers, without prior written approval of the individual identified in Block 17 of this form.

The classification assigned to a particular stage in the contractual process does not mean that everything applicable to that stage is to be given the same classification. Every item shall be PROTECTED and/or CLASSIFIED according to its own content. If a supplier is in doubt as to the actual level to be assigned, they should consult with the individual identified in Block 17 of this form.

PART A - CONTRACT INFORMATION

Contract Number (top of the form)
This number must be the same as that found on the requisition and should be the one used when issuing an RFP or contract. This is a unique number (i.e. no two requirements will have the same number). A new SRCL must be used for each new requirement or requisition (e.g. new contract number, new SRCL, new signatures).

1. Originating Government Department or Organization
Enter the department or client organization name or the prime contractor name for which the work is being performed.

2. Directorate / Branch
This block is used to further identify the area within the department or organization for which the work will be conducted.

3. a) Subcontract Number
If applicable, this number corresponds to the number generated by the Prime Contractor to manage the work with its subcontractor.

b) Name and Address of Subcontractor
Indicate the full name and address of the Subcontractor if applicable.

4. Brief Description of Work
Provide a brief explanation of the nature of the requirement or work to be performed.

5. a) Will the supplier require access to Controlled Goods?
The Defence Production Act (DPA) defines "Controlled Goods" as certain goods listed in the Export Control List, a regulation made pursuant to the *Export and Import Permits Act* (EIPA). Suppliers who examine, possess, or transfer Controlled Goods within Canada must register in the Controlled Goods Directorate or be exempt from registration. More information may be found at www.cgd.gc.ca.

b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?
The prime contractor and any subcontractors must be certified under the U.S./Canada Joint Certification Program if the work involves access to unclassified military data subject to the provisions of the Technical Data Control Regulations. More information may be found at www.dlis.dla.mil/jcp.

6. Indicate the type of access required

Identify the nature of the work to be performed for this requirement. The user is to select one of the following types:

a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?

The supplier would select this option if they require access to PROTECTED and/or CLASSIFIED information or assets to perform the duties of the requirement.

b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.

The supplier would select this option if they require regular access to government premises or a secure work site only. The supplier will not have access to PROTECTED and/or CLASSIFIED information or assets under this option.

c) Is this a commercial courier or delivery requirement with no overnight storage?

The supplier would select this option if there is a commercial courier or delivery requirement. The supplier will not be allowed to keep a package overnight. The package must be returned if it cannot be delivered.

7. Type of information / Release restrictions / Level of information

Identify the type(s) of information that the supplier may require access to, list any possible release restrictions, and if applicable, provide the level(s) of the information. The user can make multiple selections based on the nature of the work to be performed.

Departments must process SRCLs through PWGSC where:

- contracts that afford access to PROTECTED and/or CLASSIFIED foreign government information and assets;
- contracts that afford foreign contractors access to PROTECTED and/or CLASSIFIED Canadian government information and assets; or
- contracts that afford foreign or Canadian contractors access to PROTECTED and/or CLASSIFIED information and assets as defined in the documents entitled Identifying INFOSEC and INFOSEC Release.

a) Indicate the type of information that the supplier will be required to access

Canadian government information and/or assets

If Canadian information and/or assets are identified, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by the Canadian government.

NATO information and/or assets

If NATO information and/or assets are identified, this indicates that as part of this requirement, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by NATO governments. NATO information and/or assets are developed and/or owned by NATO countries and are not to be divulged to any country that is not a NATO member nation. Persons dealing with NATO information and/or assets must hold a NATO security clearance and have the required need-to-know.

Requirements involving CLASSIFIED NATO information must be awarded by PWGSC. PWGSC / CIISD is the Designated Security Authority for industrial security matters in Canada.

Foreign government information and/or assets

If foreign information and/or assets are identified, this requirement will allow access to information and/or assets owned by a country other than Canada.

b) Release restrictions

If **Not Releasable** is selected, this indicates that the information and/or assets are for **Canadian Eyes Only (CEO)**. Only Canadian suppliers based in Canada can bid on this type of requirement. NOTE: If Canadian information and/or assets coexists with CEO information and/or assets, the CEO information and/or assets must be stamped **Canadian Eyes Only (CEO)**.

If **No Release Restrictions** is selected, this indicates that access to the information and/or assets are not subject to any restrictions.

If **ALL NATO countries** is selected, bidders for this requirement must be from NATO member countries only.

NOTE: There may be multiple release restrictions associated with a requirement depending on the nature of the work to be performed. In these instances, a security guide should be added to the SRCL clarifying these restrictions. The security guide is normally generated by the organization's project authority and/or security authority.

c) Level of information

Using the following chart, indicate the appropriate level of access to information/assets the supplier must have to perform the duties of the requirement.

PROTECTED	CLASSIFIED	NATO
PROTECTED A	CONFIDENTIAL	NATO UNCLASSIFIED
PROTECTED B	SECRET	NATO RESTRICTED
PROTECTED C	TOP SECRET	NATO CONFIDENTIAL
	TOP SECRET (SIGINT)	NATO SECRET
		COSMIC TOP SECRET

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
If Yes, the supplier personnel requiring access to COMSEC information or assets must receive a COMSEC briefing. The briefing will be given to the "holder" of the COMSEC information or assets. In the case of a "personnel assigned" type of contract, the customer department will give the briefing. When the supplier is required to receive and store COMSEC information or assets on the supplier's premises, the supplier's COMSEC Custodian will give the COMSEC briefings to the employees requiring access to COMSEC information or assets. If Yes, the Level of sensitivity must be indicated.

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
If Yes, the supplier must provide the Short Title of the material and the Document Number. Access to extremely sensitive INFOSEC information or assets will require that the supplier undergo a Foreign Ownership Control or Influence (FOCI) evaluation by CIISD.

PART B - PERSONNEL (SUPPLIER)

10. a) Personnel security screening level required

Identify the screening level required for access to the information/assets or client facility. More than one level may be identified depending on the nature of the work. Please note that Site Access screenings are granted for access to specific sites under prior arrangement with the Treasury Board of Canada Secretariat. A Site Access screening only applies to individuals, and it is not linked to any other screening level that may be granted to individuals or organizations.

RELIABILITY STATUS	CONFIDENTIAL	SECRET
TOP SECRET	TOP SECRET (SIGINT)	NATO CONFIDENTIAL
NATO SECRET	COSMIC TOP SECRET	SITE ACCESS

If multiple levels of screening are identified, a Security Classification Guide must be provided.

b) May unscreened personnel be used for portions of the work?

Indicating Yes means that portions of the work are not PROTECTED and/or CLASSIFIED and may be performed outside a secure environment by unscreened personnel. The following question must be answered if unscreened personnel will be used:

Will unscreened personnel be escorted?

If No, unscreened personnel may not be allowed access to sensitive work sites and must not have access to PROTECTED and/or CLASSIFIED information and/or assets.

If Yes, unscreened personnel must be escorted by an individual who is cleared to the required level of security in order to ensure there will be no access to PROTECTED and/or CLASSIFIED information and/or assets at the work site.

PART C - SAFEGUARDS (SUPPLIER)

11. INFORMATION / ASSETS

a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information and/or assets on its site or premises?

If Yes, specify the security level of the documents and/or equipment that the supplier will be required to safeguard at their own site or premises using the summary chart.

b) Will the supplier be required to safeguard COMSEC information or assets?

If Yes, specify the security level of COMSEC information or assets that the supplier will be required to safeguard at their own site or premises using the summary chart.

PRODUCTION

c) Will the production (manufacture, repair and/or modification) of PROTECTED and/or CLASSIFIED material and/or equipment occur at the supplier's site or premises?

Using the summary chart, specify the security level of material and/or equipment that the supplier manufactured, repaired and/or modified and will be required to safeguard at their own site or premises.

INFORMATION TECHNOLOGY (IT)

d) Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data?

If Yes, specify the security level in the summary chart. This block details the information and/or data that will be electronically processed or produced and stored on a computer system. The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. The supplier must also direct their attention to the following document: Treasury Board of Canada Secretariat - Operational Security Standard: Management of Information Technology Security (MITS).

e) Will there be an electronic link between the supplier's IT systems and the government department or agency?

If Yes, the supplier must have their IT system(s) approved. The Client Department must also provide the Connectivity Criteria detailing the conditions and the level of access for the electronic link (usually not higher than PROTECTED B level).

SUMMARY CHART

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.

For users completing the form **online** (via the Internet), the Summary Chart is automatically populated by your responses to previous questions.

PROTECTED	CLASSIFIED	NATO	COMSEC
PROTECTED A	CONFIDENTIAL	NATO RESTRICTED	PROTECTED A
PROTECTED B	SECRET	NATO CONFIDENTIAL	PROTECTED B
PROTECTED C	TOP SECRET	NATO SECRET	PROTECTED C
	TOP SECRET (SIGINT)	COSMIC TOP SECRET	CONFIDENTIAL
			SECRET
			TOP SECRET

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".

b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).

PART D - AUTHORIZATION

13. Organization Project Authority

This block is to be completed and signed by the appropriate project authority within the client department or organization (e.g. the person responsible for this project or the person who has knowledge of the requirement at the client department or organization). This person may on occasion be contacted to clarify information on the form.

14. Organization Security Authority

This block is to be signed by the Departmental Security Officer (DSO) (or delegate) of the department identified in Block 1, or the security official of the prime contractor.

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?

A Security Guide or Security Classification Guide is used in conjunction with the SRCL to identify additional security requirements which do not appear in the SRCL, and/or to offer clarification to specific areas of the SRCL.

16. Procurement Officer

This block is to be signed by the procurement officer acting as the contract or subcontract manager.

17. Contracting Security Authority

This block is to be signed by the Contract Security Official. Where PWGSC is the Contract Security Authority, Canadian and International Industrial Security Directorate (CIISD) will complete this block.

Instructions pour établir la Liste de vérification des exigences relatives à la sécurité (LVERS)

La feuille d'instructions devrait rester jointe au formulaire jusqu'à ce que la case 17 ait été remplie.

GÉNÉRALITÉS - TRAITEMENT DU PRÉSENT FORMULAIRE

Le responsable du projet doit faire remplir ce formulaire.

L'agent de sécurité de l'organisation doit revoir et approuver les exigences de sécurité qui figurent dans le formulaire, en collaboration avec le responsable du projet.

Le responsable de la sécurité des marchés est le responsable chargé de voir à ce que les fournisseurs se conforment aux exigences de sécurité mentionnées dans la LVERS.

Toutes les demandes d'achat ainsi que tous les appels d'offres et les documents contractuels subséquents, y compris les contrats de sous-traitance, qui comprennent des exigences relatives à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS doivent être accompagnés d'une LVERS dûment remplie.

Il importe d'indiquer si les renseignements ou les biens PROTÉGÉS sont de niveau A, B ou C, le cas échéant; cependant, certains types de renseignements peuvent être indiqués par la mention « PROTÉGÉ » seulement. Aucun renseignement relatif à un contrat gouvernemental PROTÉGÉ ou CLASSIFIÉ ne peut être divulgué par les fournisseurs sans l'approbation écrite préalable de la personne dont le nom figure à la case 17 de ce formulaire.

La classification assignée à un stade particulier du processus contractuel ne signifie pas que tout ce qui se rapporte à ce stade doit recevoir la même classification. Chaque article doit être PROTÉGÉ et/ou CLASSIFIÉ selon sa propre nature. Si un fournisseur ne sait pas quel niveau de classification assigner, il doit consulter la personne dont le nom figure à la case 17 de ce formulaire.

PARTIE A - INFORMATION CONTRACTUELLE

Numéro du contrat (au haut du formulaire)
Ce numéro doit être le même que celui utilisé sur la demande d'achat et services et devrait être celui utilisé dans la DDP ou dans le contrat. Il s'agit d'un numéro unique (c.-à-d. que le même numéro ne sera pas attribué à deux besoins distincts). Une nouvelle LVERS doit être utilisée pour chaque nouveau besoin ou demande (p. ex. un nouveau numéro de contrat, une nouvelle LVERS, de nouvelles signatures).

1. Ministère ou organisme gouvernemental d'origine
Inscrire le nom du ministère ou de l'organisme client ou le nom de l'entrepreneur principal pour qui les travaux sont effectués.

2. Direction générale ou Direction
Cette case peut servir à fournir plus de détails quant à la section du ministère ou de l'organisme pour qui les travaux sont effectués.

3. a) Numéro du contrat de sous-traitance
S'il y a lieu, ce numéro correspond au numéro généré par l'entrepreneur principal pour gérer le travail avec son sous-traitant.

b) Nom et adresse du sous-traitant
Indiquer le nom et l'adresse au complet du sous-traitant, s'il y a lieu.

4. Brève description du travail
Donner un bref aperçu du besoin ou du travail à exécuter.

5. a) Le fournisseur aura-t-il accès à des marchandises contrôlées?
La *Loi sur la production de défense* (LPD) définit « marchandises contrôlées » comme désignant certains biens énumérés dans la Liste des marchandises d'exportation contrôlée, un règlement établi en vertu de la *Loi sur les licences d'exportation et d'importation* (LLEI). Les fournisseurs qui examinent, possèdent ou transfèrent des marchandises contrôlées à l'intérieur du Canada doivent s'inscrire à la Direction des marchandises contrôlées ou être exemptés de l'inscription. On trouvera plus d'information à l'adresse www.cgp.gc.ca.

b) Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?
L'entrepreneur et tout sous-traitant doivent être accrédités en vertu du Programme mixte d'agrément Etats-Unis / Canada si le travail comporte l'accès à des données militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques. On trouvera plus d'information à l'adresse www.dlis.dla.mil/jcp/.

6. Indiquer le type d'accès requis

Indiquer la nature du travail à exécuter pour répondre à ce besoin. L'utilisateur doit choisir un des types suivants :

a) Le fournisseur et ses employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?

Le fournisseur choisit cette option s'il doit avoir accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS pour accomplir le travail requis.

b) Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.

Le fournisseur choisit cette option seulement s'il doit avoir accès régulièrement aux locaux du gouvernement ou à un lieu de travail protégé. Le fournisseur n'aura pas accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS en vertu de cette option.

c) S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?

Le fournisseur choisit cette option s'il y a nécessité de recourir à un service de messagerie ou de livraison commerciale. Le fournisseur ne sera pas autorisé à garder un colis pendant la nuit. Le colis doit être retourné s'il ne peut pas être livré.

7. Type d'information / Restrictions relatives à la diffusion / Niveau d'information

Indiquer le ou les types d'information auxquels le fournisseur peut devoir avoir accès, énumérer toutes les restrictions possibles relatives à la diffusion, et, s'il y a lieu, indiquer le ou les niveaux d'information. L'utilisateur peut faire plusieurs choix selon la nature du travail à exécuter.

Les ministères doivent soumettre la LVERS à TPSGC lorsque:

- les marchés prévoient l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS étrangers ;
- les marchés prévoient aux entrepreneurs étrangers l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS canadiens; ou
- les marchés prévoient aux entrepreneurs étrangers ou canadiens l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS tels que définis dans les documents intitulés Moyens INFOSEC détermination et Divulgation de INFOSEC.

a) Indiquer le type d'information auquel le fournisseur devra avoir accès

Renseignements et/ou biens du gouvernement canadien

Si des renseignements et/ou des biens canadiens sont indiqués, le fournisseur aura accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS appartenant au gouvernement canadien.

Renseignements et/ou biens de l'OTAN

Si des renseignements et/ou des biens de l'OTAN sont indiqués, cela signifie que, dans le cadre de ce besoin, le fournisseur aura accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS appartenant à des gouvernements membres de l'OTAN. Les renseignements et/ou les biens de l'OTAN sont élaborés par des pays de l'OTAN ou leur appartiennent et ne doivent être divulgués à aucun pays qui n'est pas un pays membre de l'OTAN. Les personnes qui manient des renseignements et/ou des biens de l'OTAN doivent détenir une autorisation de sécurité de l'OTAN et avoir besoin de savoir.

Les contrats comportant des renseignements CLASSIFIÉS de l'OTAN doivent être attribués par TPSGC. La DSICI de TPSGC est le responsable de la sécurité désigné relativement aux questions de sécurité industrielle au Canada.

Renseignements et/ou biens de gouvernements étrangers

Si des renseignements et/ou des biens de gouvernements étrangers sont indiqués, ce besoin permettra l'accès à des renseignements et/ou à des biens appartenant à un pays autre que le Canada.

b) Restrictions relatives à la diffusion

Si **À ne pas diffuser** est choisi, cela indique que les renseignements et/ou les biens sont **réservés aux Canadiens**. Seuls des fournisseurs canadiens installés au Canada peuvent soumissionner ce genre de besoin. NOTA : Si des renseignements et/ou des biens du gouvernement canadien coexistent avec des renseignements et/ou des biens réservés aux Canadiens, ceux-ci doivent porter la mention **Réservé aux Canadiens**.

Si **Aucune restriction relative à la diffusion** est choisi, cela indique que l'accès aux renseignements et/ou aux biens n'est assujetti à aucune restriction.

Si **Tous les pays de l'OTAN** est choisi, les soumissionnaires doivent appartenir à un pays membre de l'OTAN.

NOTA : Il peut y avoir plus d'une restriction s'appliquant à une demande, selon la nature des travaux à exécuter. Pour ce genre de contrat, un guide de sécurité doit être joint à la LVERS afin de clarifier les restrictions. Ce guide est généralement préparé par le chargé de projet et/ou le responsable de la sécurité de l'organisme.

c) Niveau d'information

À l'aide du tableau ci-dessous, indiquer le niveau approprié d'accès aux renseignements et/ou aux biens que le fournisseur doit avoir pour accomplir les travaux requis.

PROTÉGÉ	CLASSIFIÉ	NATO
PROTÉGÉ A	CONFIDENTIEL	NATO NON CLASSIFIÉ
PROTÉGÉ B	SECRET	NATO DIFFUSION RESTREINTE
PROTÉGÉ C	TRÈS SECRET	NATO CONFIDENTIEL
	TRÈS SECRET (SIGINT)	NATO SECRET
		COSMIC TRÈS SECRET

8. Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?
Si la réponse est Oui, les membres du personnel du fournisseur qui doivent avoir accès à des renseignements ou à des biens COMSEC doivent participer à une séance d'information COMSEC. Cette séance sera donnée au « détenteur autorisé » des renseignements ou des biens COMSEC. Dans le cas des contrats du type « personnel affecté », cette séance sera donnée par le ministère client. Lorsque le fournisseur doit recevoir et conserver, dans ses locaux, des renseignements ou des biens COMSEC, le responsable de la garde des renseignements ou des biens COMSEC de l'entreprise donnera la séance d'information COMSEC aux membres du personnel qui doivent avoir accès à des renseignements ou à des biens COMSEC.

9. Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?
Si la réponse est Oui, le fournisseur doit indiquer le titre abrégé du document, le numéro du document et le niveau de sensibilité. L'accès à des renseignements ou à des biens extrêmement délicats INFOSEC exigera que le fournisseur fasse l'objet d'une vérification Participation, contrôle et influence étrangers (PCIE) effectuée par la DSICI.

PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Niveau de contrôle de la sécurité du personnel requis

Indiquer le niveau d'autorisation de sécurité que le personnel doit détenir pour avoir accès aux renseignements, aux biens ou au site du client. Selon la nature du travail, il peut y avoir plus d'un niveau de sécurité. Veuillez noter que des cotes de sécurité sont accordées pour l'accès à des sites particuliers, selon des dispositions antérieures prises auprès du Secrétariat du Conseil du Trésor du Canada. La cote de sécurité donnant accès à un site s'applique uniquement aux personnes et n'est liée à aucune autre autorisation de sécurité accordée à des personnes ou à des organismes.

COTE DE FIABILITÉ	CONFIDENTIEL	SECRET
TRÈS SECRET	TRÈS SECRET (SIGINT)	NATO CONFIDENTIEL
NATO SECRET	COSMIC TRÈS SECRET	ACCÈS AUX EMPLACEMENTS

Si plusieurs niveaux d'autorisation de sécurité sont indiqués, un guide de classification de sécurité doit être fourni.

b) Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

Si la réponse est Oui, cela veut dire que certaines tâches ne sont pas PROTÉGÉES et/ou CLASSIFIÉES et peuvent être exécutées à l'extérieur d'un environnement sécurisé par du personnel n'ayant pas d'autorisation de sécurité. Il faut répondre à la question suivante si l'on a recours à du personnel n'ayant pas d'autorisation de sécurité :

Le personnel n'ayant pas d'autorisation de sécurité sera-t-il escorté?

Si la réponse est Non, le personnel n'ayant pas d'autorisation de sécurité ne pourra pas avoir accès à des lieux de travail dont l'accès est réglementé ni à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS.

Si la réponse est Oui, le personnel n'ayant pas d'autorisation de sécurité devra être escorté par une personne détenant la cote de sécurité requise, pour faire en sorte que le personnel en question n'ait pas accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS sur les lieux de travail.

PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

11. RENSEIGNEMENTS / BIENS :

a) Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, préciser, à l'aide du tableau récapitulatif, le niveau de sécurité des documents ou de l'équipement que le fournisseur devra protéger dans ses installations.

b) Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

Si la réponse est Oui, préciser, à l'aide du tableau récapitulatif, le niveau de sécurité des renseignements ou des biens COMSEC que le fournisseur devra protéger dans ses installations.

PRODUCTION

c) Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

Préciser, à l'aide du tableau récapitulatif, le niveau de sécurité du matériel que le fournisseur fabriquera, réparera et/ou modifiera et devra protéger dans ses installations.

TECHNOLOGIE DE L'INFORMATION (TI)

d) Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, préciser le niveau de sécurité à l'aide du tableau récapitulatif. Cette case porte sur les renseignements qui seront traités ou produits électroniquement et stockés dans un système informatique. Le ministère/organisme client devra préciser les exigences en matière de sécurité de la TI relativement à cet achat dans un document technique distinct. Le fournisseur devra également consulter le document suivant : Secrétariat du Conseil du Trésor du Canada – Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).

e) Y aura-t-il un lien électronique entre les systèmes informatiques du fournisseur et celui du ministère ou de l'agence gouvernementale?

Si la réponse est Oui, le fournisseur doit faire approuver ses systèmes informatiques. Le ministère client doit aussi fournir les critères de connectivité qui décrivent en détail les conditions et le niveau de sécurité relativement au lien électronique (habituellement pas plus haut que le niveau PROTÉGÉ B).

TABLEAU RÉCAPITULATIF

Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

PROTÉGÉ	CLASSIFIÉ	NATO	COMSEC
PROTÉGÉ A	CONFIDENTIEL	NATO DIFFUSION RESTREINTE	PROTÉGÉ A
PROTÉGÉ B	SECRET	NATO CONFIDENTIEL	PROTÉGÉ B
PROTÉGÉ C	TRÈS SECRET	NATO SECRET	PROTÉGÉ C
	TRÈS SECRET (SIGINT)	COSMIC TRÈS SECRET	CONFIDENTIEL
			SECRET
			TRÈS SECRET

12. a) La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

Si la réponse est Oui, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de

sécurité » au haut et au bas du formulaire.

b) La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

Si la réponse est Oui, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

PARTIE D - AUTORISATION

13. Chargé de projet de l'organisme

Cette case doit être remplie et signée par le chargé de projet pertinent (c.-à-d. la personne qui est responsable de ce projet ou qui connaît le besoin au ministère ou à l'organisme client. On peut, à l'occasion, communiquer avec cette personne pour clarifier des renseignements figurant sur le formulaire.

14. Responsable de la sécurité de l'organisme

Cette case doit être signée par l'agent de la sécurité du ministère (ASM) du ministère indiqué à la case 1 ou par son remplaçant ou par le responsable de la sécurité du fournisseur.

15. Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

Un Guide de sécurité ou un Guide de classification de sécurité sont utilisés de concert avec la LVERS pour faire part d'exigences supplémentaires en matière de sécurité qui n'apparaissent pas dans la LVERS et/ou pour éclaircir certaines parties de la LVERS.

16. Agent d'approvisionnement

Cette case doit être signée par l'agent des achats qui fait fonction de gestionnaire du contrat ou du contrat de sous-traitance.

17. Autorité contractante en matière de sécurité

Cette case doit être signée par l'agent de la sécurité du marché. Lorsque TPSGC est le responsable de la sécurité du marché, la Direction de la sécurité industrielle canadienne et internationale (DSICI) doit remplir cette case.

Shared Services Canada

Conferencing & Operator Assisted Service (COAS)

Annex F – Security Obligations for Commercial Cloud Services

Version 1.0

Table of Contents

1 General

1.1 Purpose

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

1.2 Flow-Down of Security Obligations

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

1.3 Change Management

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

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

2 Acknowledgments

The parties acknowledge that:

a) Canada's Data is subject to these Security Obligations.
b) Notwithstanding any other provision of this Annex, the parties have shared responsibility for developing and maintaining policies, procedures and security controls relating to Canada's Data.
c) The Contractor must not have or attempt to gain custody of Canada's Data, nor permit any Cloud Services Personnel to access Canada's Data prior to the implementation of the Security Requirements as required under this Annex on or before Contract Award.
d) Security Obligations apply to **Commercial Cloud Services** up to and including Protected A / Low Integrity, Low Availability or Low Injury, unless otherwise specified.

3 Securing Canada's Data

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

4 Roles and Responsibilities for Security

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

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

5 Third-Party Assurance: Certifications and Reports

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

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

a) ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Certification achieved by an accredited certification body (or subsequent versions); OR
b) 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; AND
c) Contractor's self-assessment to Cloud Security Alliance Cloud Controls Matrix (CCM) v4 (or subsequent versions).

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

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

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

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

6 Auditing Compliance

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

a) Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;
b) Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework; and
c) Each audit will be performed by independent, third-party auditors that (i) are qualified under the AICPA, CPA Canada, or ISO certification regime, and (ii) conform to the ISO/IEC 17020 quality management system standard at the Contractor's selection and expense.

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

Upon request of Canada, additional supplementary evidence from the Contractor, including system security plans, designs, or architecture documents that provide a comprehensive system description, may be provided by the Contractor or a Sub-processor to supplement the certification and audit reports described in Section 5 (Third Party Assurance) to demonstrate the Contractor's compliance with the required industry certifications. This includes the situation where the Contractor is a SaaS or PaaS provider using physical data centers that are provided by a third-party IaaS provider.

7 Cloud Service Provider (CSP) IT Security Assessment Program

The Contractor must demonstrate compliance with the security requirements selected in the Canadian Centre for Cyber Security (CCCS) Annex A Cloud Control Profile – Low 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 Contractor. Compliance must be demonstrated through the mapping of security controls to the applicable industry certifications identified below and validated through independent third-party assessments.

Compliance will be assessed and validated through the CCCS 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).

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

a) A copy of the most recent completed assessment report provided by Canada; and
b) A copy of the most recent summary report provided by Canada.
c) The Contractor should contact the procuring GC department for any additional information related to the CSP IT Assessment Program.
d) It is the continuous obligation of the Contractor of the proposed Cloud Services to notify GC procuring department when there are significant changes to its delivery of the IT Security services supporting the Contractor offering.

In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with Section 5 - Third-Party Assurance and Section 7 - Cloud Service Provider (CSP) IT Security Assessment Program, sub-sections (1) and (2) the SaaS provider must provide Canada with a copy of an email provided by the Canadian Centre for Cyber Security (CCCS) confirming that the Bidder has completed the CCCS CSP ITS Assessment Program. The email must state that the CSP has been assessed by the CSP ITS Assessment Program and that the CSP has received a final report with regards to the assessment. For any questions, CCCS can be contacted by email at contact@cyber.gc.ca.

8 Data Protection

The Contractor must:

a) Implement encryption of data at rest for the Cloud Services hosting Canada's Data where the encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure, in accordance with Section 13 - Cryptographic Protection.
b) Transmit Canada's Data in a secure manner including ability for the GC to implement encryption for data in transit for all transmissions of Canada's Data, in accordance with Section 13 - Cryptographic Protection and Section 21- Network and Communications Security.

The Contractor must:

a) Implement security controls that restricts administrative access to Canada's Data and Systems by the Contractor and provides the ability to require the written approval of Canada before the Contractor can access Canada's Data to perform support, maintenance or operational activities
b) Take reasonable measures to ensure that Contractor Personnel do not have standing or ongoing access rights to Canada's Data, and access is restricted to Contractor Personnel with a need-to-know, including resources that provide technical or customer support, based on approval from Canada.

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

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

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

9 Data Segregation

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

a) The separation between Contractor's internal administration from resources used by its customers;
b) The separation of customer resources in multi-tenant environments in order to prevent one malicious or compromised consumer from affecting the service or data of another; and
c) (For IaaS) Ability for the GC to support isolation within GC-managed tenant environment.

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

10 Data Location

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

a) A data centre that meets all security requirements and certifications identified in Section 30 for Physical (Data Centre / Facilities) Security;
b) Ensures the infeasibility of finding a specific customer's data on physical media; and
c) Employs encryption to ensure that no data is written to disk in an unencrypted form, in accordance with Section 13 - Cryptographic Protection.

Upon request of Canada, the Contractor must:

a) Provide the GC with an up-to-date list of the physical locations, including city, which may contain Canada's Data for each data centre that will be used to provide the Cloud services; and
b) Identify which portions of the Cloud Services are delivered from outside of Canada, including all locations where data is stored and processed and where the Contractor manages the service from.

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

11 Data Transfer and Retrieval

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

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

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

12 Data Disposition and Returning Records to Canada

The Contractor must securely dispose or reuse resources (e.g., equipment, data storage, files, and memory) that contain Canada's Data and ensure that previously stored data cannot be accessed by other customers after it is released. This includes all copies of Canada's Data that are made through replication for high availability and disaster recovery. The Contractor's disposal or reuse of resources must be aligned with one of the following:

a) National Industrial Security Program Operating Manual (DoD 5220.22-M6); (ii) Guidelines for Media Sanitization (NIST SP 800-88); or (iii) Clearing and Declassifying Electronic Data Storage Devices (CSE ITSG-06). Upon request of Canada, the Contractor must provide a document that describes the Contractor's process for disposal or reuse of resources.

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

13 Cryptographic Protection

The Contractor must:

a) Configure any cryptography used to implement confidentiality or integrity safeguards, or used as part of an authentication mechanism (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable), in accordance with Communications Security Establishment (CSE)-approved cryptographic algorithms and cryptographic parameter sizes, key lengths and key crypto periods as specified in "Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information" (ITSP.40.111) and "Guidance on Securely Configuring Network Protocols" (ITSP.40.062) and remain consistent with any subsequent versions published on https://cyber.gc.ca/;

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

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

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

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

14 Key Management

The Contractor must provide Canada with a key management service aligned with CCCS Guidance on cloud service cryptography (ITSP.50.106) - Canadian Centre for Cyber Security and their subsequent versions published on https://cyber.gc.ca/, that includes:

a) Ability to create/generate and delete encryption keys if required by the GC.
b) Definition and application of specific policies that control how keys can be used;
c) Protection of access to the key material including prevention from Contractor access to the key material in unencrypted fashion;
d) Ability to audit all events related to key management services, including Contractor access for Canada's review;
e) Ability to securely import GC generated keys from GC-managed on-premise hardware security module (HSM) without exposure of key plaintext during the import process;
f) Ability to prevent the Cloud Service Provider to recover plaintext copies of the GC generated keys; and
g) Ability to delegate key use privileges for use by the Cloud Services used for the GC managed services.

15 Endpoint Protection

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

16 Secure Development

The Contractor must implement a software and system development lifecycle that applies information system security engineering principles throughout the information system life cycle and in the development of software and websites and services, and conforms to industry standards and best practices, such as

a) NIST,

b) ISO 27034,

c) ITSG-33,

d) SAFECode, or

e) Open Web Application Security Project (OWASP) standards such as Application Security Verification Standard (ASVS) or an equivalent standard approved by Canada in writing.

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

17 Identity and Access Management

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

a) Phishing-resistant multi-factor authentication in accordance with CSE's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) using GC-approved credentials;
b) Role-based access;
c) Access controls on objects in storage; and
d) Granular authorization policies to allow or limit access.

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

18 Federation

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

a) Support for open standards for authentication protocols such as Security Assertion Markup Language (SAML) 2.0 (or subsequent versions) and OpenID Connect 1.0 (or subsequent versions) where the End User credentials and authentication to cloud services are under the sole control of Canada; and
b) Ability to associate Canada unique identifiers (e.g. a Canada unique ID, a Canada email address, etc.) with the corresponding Cloud Service user account(s).

19 Privileged Access Management

The Contractor must:

a) Implement access control policies and procedures that address onboarding, off- boarding, transition between roles, regular access reviews to identify excessive privileges, limitations and usage control of administrator privileges;
b) Manage and monitor privileged access to the Cloud Services to ensure that all service interfaces within a multi-tenant environment are protected from unauthorized access, including those that are used to host GC services;
c) Restrict and minimize access to the Cloud Services and Canada's Data to only authorized devices and End Users with an explicit need to have access;
d) Enforce and audit authorizations for access to the Cloud Services and Canada's Data;
e) Constrain all access to service interfaces that host Canada's Data to uniquely identified, authenticated and authorized End Users, devices, and processes (or services);
f) Implement password policies to protect credentials from compromise by either online or off-line attacks and to detect these attacks by logging and monitoring events such as (i) successful use of credentials, (ii) unusual use of credential, and (iii) access to and exfiltration from the password database, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);
g) Implement multi-factor authentication mechanisms to authenticate End Users with privileged access, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);
h) Implement role-based access control mechanisms to assign privileges which form the basis to enforce access to Canada's Data;
i) Define and implement separation of duties to achieve, at a minimum, separation of service management and administration roles from information system support roles, development roles from operational roles, and access management roles from other operational roles;
j) Adhere to the principles of least privilege and need-to-know when granting access to the Cloud Services and Canada's Data;
k) Use security-hardened endpoints (e.g., computers, end user devices, jump servers, etc.) that are configured for least functionality (e.g., dedicated endpoint that does not have Internet browsing or open e-mail access) to provide support and administration of Cloud Services and Contractor Infrastructure;
l) Implement an automated process to periodically audit, at a minimum, account creation, modification, enabling, disabling, and removal actions; and
m) Upon termination of employment, terminate or revoke authenticators and access credentials associated with any Services Personnel.

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

20 Remote Management

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

a) Implement multi-factor authentication mechanisms for authenticate remote access users, in accordance with CCCS's ITSP.30.031 V3 (or subsequent versions) (https://cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3);
b) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions, in accordance with Section 13 (Cryptographic Protection);
c) Route all remote access through controlled, monitored, and audited access control points;
d) Expeditiously disconnect or disable unauthorized remote management or remote access connections;
e) Authorize remote execution of privileged commands and remote access to security-relevant information.

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

21 Network and Communications Security

The Contractor must:

a) Provide the ability for Canada to establish secure connections to the Cloud Services, including providing data-in-transit protection between Canada and the Cloud Service using TLS 1.2, or subsequent versions;
b) Use up-to-date and supported protocols, cryptographic algorithms and certificates, as outlined in CCCS's ITSP.40.062 (https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) and ITSP.40.111 (https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111);
c) Use correctly configured certificates within the TLS connections in accordance with CCCS guidance.
d) Provide the ability for Canada to implement network access controls and security rules that restrict access to only authorized devices and network locations to Canada resources.

22 Logging and Auditing

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

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

a) log and detect audit events such as (i) successful and unsuccessful account login attempts, (ii) account management, (iii) object access and policy change, (iv) privilege functions and process tracking, (v) system events, (vi) deletion of data, and in accordance with Canada's Event Logging Guidance (https://www.canada.ca/en/government/system/digital-government/online- security-privacy/event-logging-guidance.html);
b) record in logs (or log files) audit events that are time synchronized and timestamped in coordinated universal time (UTC) and protected from unauthorized access, modification, or deletion while in transit and at rest;
c) provide real-time alerts of failed audit events to personnel with the authority to address the failed audit events; and
d) separate Security Incidents and logs for different Canada accounts to enable Canada to monitor and manage events within its boundary that are affecting its instance of an IaaS, PaaS or SaaS Cloud Service provided to it by the Contractor or a Sub-processor.

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

For SaaS, the Contractor must provide APIs that provide the ability to:

a) Inspect and interrogate data at rest in SaaS applications;
b) Assess events such as user access and behavior, administrator access and behavior, and changes to third-party API access, stored in SaaS application logs.

23 Continuous Monitoring

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

a) Actively and continuously monitor threats and vulnerabilities to Contractor Infrastructure, Service Locations, or Canada's Data;
b) Conduct regular vulnerability scans and penetration testing of the Contractor Infrastructure and Service Locations, with the aim of identifying deficiencies and remediations to prevent unauthorized access to sensitive information, circumvention of access controls and privilege escalation, and exploitation of vulnerabilities to gain access to systems or information.
c) Undertake best efforts to prevent attacks through security measures such as denial of service protections;
d) Undertake best efforts to detect attacks, Security Incidents, and other abnormal events;
e) Identify unauthorized use and access of any Cloud Services, data, and components relevant to Canada's IaaS, PaaS or SaaS Cloud Service;
f) Manage and apply security-related patches and updates in a timely and systematic manner to mitigate vulnerabilities and remedy any publicly reported issues in the Cloud Services or libraries that the Cloud Services make use of, and provide advance notices of patches in accordance with agreed-upon service level commitments;
g) Respond, contain, and recover from threats and attacks against the Contractor Cloud Services; and
h) Where required, take proactive countermeasures, including taking both preemptive and responsive actions, to mitigate threats.

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

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

24 Security Incident Management

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

a) A published and documented Security Incident Response Process for review by Canada that is aligned with one of the following standards: (i) ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management; or (ii) NIST SP800-612, Computer Security Incident Handling Guide; or (iii) GC Cyber Security Event Management Plan (GC CSEMP) (https://www.canada.ca/en/government/system/digital-government/online- security-privacy/security-identity-management/government-canada-cyber- security-event-management-plan.html); or (iv) other best practices from industry standards, if Canada determines, in its discretion, that they meet Canada's security requirements.

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

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

d) Allows only designated, pre-authorized representatives of Customer (e.g., Canadian Centre for Cyber Security, or other GC-approved organizations) authorized by the Technical Authority:
   i. to request and receive discrete access and information associated with Customer's Data (user data, system/security event logs, network or host packet captures, logs from security components such as IDS/IPS/Firewalls, etc.), in an unencrypted fashion, for the purposes of conducting investigations;
   ii. the ability for Customer to track the status of a reported information security event.

e) Procedures to respond to requests for potential digital evidence or other information from within the Cloud Services environment and conforms to industry standards and best practices including ISO 22095:2020 Chain of custody — General terminology and models (https://www.iso.org/standard/72532.html) including proper forensic procedures and safeguards for:
   i. the maintenance of a chain of custody for both the audit information, and
   ii. the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.

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

The Contractor must:

a) Work with Canada's Security Operations Center(s) (e.g. GC SOC, Departmental IT Security Teams) and GC CSEMP Primary Stakeholders (i.e. CCCS and Treasury Board of Canada Secretariat (TBS)), on Security Incident containment, eradication and recovery, in accordance with the Security Incident Response process and the GC CSEMP (https://www.canada.ca/en/government/system/digital-government/online-security-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html)
b) Maintain a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, the procedure for recovering data or the service, and records of activities related to the management of the security incident including internal communications and external communications (e.g., in the case of a ransomware event, all communications including ransom demands, etc.). This information must be provided to Canada upon request.; and
c) Track, or enable Canada to track, disclosure of Canada's Data, including what data has been disclosed, to whom, and at what time.

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

a) retain investigation reports related to a security investigation for a period of 2 years after the investigation is completed or provide to Canada for retention;
b) provide reasonable investigative support to designated, pre-authorized representatives of Canada such as CCCS and Royal Canadian Mounted Police (RCMP);
c) maintain chain of custody for evidence in accordance with best practices such as those outlined in ISO 22095:2020;
d) support e-discovery; and
e) maintain legal holds to meet needs of investigations and judicial requests.

In the event that the Contractor uses an external company for its incident response activities, the Contractor is expected to ensure that the provisions outlined in this *Section 25 – Security Incident Management* and *Section 26 – Security Incident Response* are also extended to the external incident response team and is documented in the Contractor's Security Incident Response Process.

25 Security Incident Response

The Contractor must alert and promptly notify Canada (via phone and email), as per the reporting procedures outlined in sub-section (25), of any compromise, breach or of any evidence such as (i) a security incident, (ii) a security malfunction in any asset, (iii) irregular or unauthorized access to any Asset, (iv) large scale copying of an Information

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

If the Contractor becomes aware of and determines a compromise or breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by the Contractor (each a "Security Incident"), the Contractor must promptly and without undue delay (i) notify Canada of the Security Incident; (ii) investigate the Security Incident and provide Canada with detailed information about the Security Incident; and (iii) take necessary steps to mitigate the cause and to minimize any damage resulting from the Security Incident.

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

26 Information Spillage

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

a) A process for identifying the specific data elements that is involved in a System's contamination;
b) A process to isolate and eradicate a contaminated System; and
c) A process for identifying Systems that may have been subsequently contaminated and any other actions performed to prevent further contamination.

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

27 Security Testing and Validation

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

a) vulnerability scans;
b) web application scans; and
c) penetration tests.

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

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

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

28 Personnel Security Screening

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

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

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

a) A description of the employee and Sub-processor positions that require access to Customer Data or could affect the confidentiality, integrity or availability of the Cloud Services;
b) A description of the security screening activities and practices, including notification procedures that need to be followed if screening has not been completed or if the results give cause for doubt or concern;
c) A description of the security awareness and training as part of employment onboarding, when employee and sub-processor roles change, and on an ongoing basis, to ensure that employees and Sub-processors understand, are aware of, and fulfil, their responsibilities for information security;
d) A description of the process that is enforced when an employee or sub-processor changes their role or when employment is terminated;
e) The approach to detecting, responding, and mitigating potential insider threats and the security controls implemented to mitigate the risk of access to GC data and/or effect on the reliability of Cloud Services hosting Canada's data.

29 Physical (Data Centre / Facilities) Security

The Contractor must implement physical security measures that ensure the protection of IT facilities and information system assets on which Canada's Data are stored and processed against all forms of tampering, loss, damage, and seizure. Physical protection of all facilities that host Canada's Data, must be applied in accordance with, or use an adequate risk-based approach based on a prevent-detect-respond-recover approach to physical security, aligned with the physical security controls and the practices in the Treasury Board Operational Security Standard on Physical Security (https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32611&section=procedure&p=C). The security measures required under this include, at a minimum:

a) Sufficient redundancy and recovery capabilities within and between the Contractor's facilities including, being geographically disparate such that the loss of one facility does not prohibit recovery of data and Canada's Data within the prescribed service level commitments;
b) Proper handling of IT Media;
c) Controlled maintenance of all information systems and their components to protect their integrity and ensure their ongoing availability;
d) Controlled access to information system output devices to prevent unauthorized access to Canada's Data;
e) Limiting physical access to Canada's Data and Service Locations to authorized Cloud Services Personnel based on position or role and the need-to-access principle, and validated by two forms of identification;
f) Escorting visitors and monitoring visitor activity;
g) Enforcing safeguarding measures for GC data at alternate work sites (e.g., telework sites);
h) Recording and monitoring all physical access to Service Locations and all logical access to Systems hosting Canada's Data, using a combination of access logs and video surveillance in all sensitive areas and intrusion detection mechanisms; and
i) Performs continuous security checks at the boundary of Service Locations and facilities for unauthorized exfiltration of information or system components.

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

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

30 Supply Chain Risk Management

The Contractor must implement safeguards to mitigate supply chain threats and vulnerabilities to IT services in order to maintain confidence in the security of the sources of information systems and the IT components used to provide Cloud Services. This includes but is not limited to protection throughout the systems development lifecycle by designing and implementing controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least privilege access for all personnel within the supply chain; threat awareness, education of the acquisition workforce on threats, risk and required security controls; and requiring supply chain entities to implement necessary safeguards.

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

a) ISO/IEC 27036 Information technology -- Security techniques -- Information security for supplier relationships (Parts 1 to 4);
b) NIST Special Publication 800-161 -- Supply Chain Risk Management Practices for Federal Information Systems and Organizations; or
c) ITSG-33 security control for SA-12 where the organization defined security safeguards are documented in an SRCM plan.

Within 90 days of contract award, the Contractor must:

a) Provide proof that the SRCM approach and plan has been independently assessed and validated by an independent third party certified under AICPA or CPA Canada, and/or ISO certification regime

OR

b) Provide Canada with a copy of the SRCM Plan on an annual basis, or upon request of Canada.

In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the Section 31 - Supply Chain Risk Management requirements, within 90 days of contract award, the SaaS provider using a GC-approved IaaS provider must provide an information communication technology (ICT) product list that describes the ICT equipment that is being deployed in the GC-approved IaaS provider environment for a supply chain integrity (SCSI) review. This SCSI review will be conducted no sooner than every three years.

31 Sub-processors

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

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

32 Industrial Security Program – Security Requirement for Canadian Suppliers

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

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

The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store PROTECTED information until written approval has been issued by the client department security authority. After approval has been granted, these tasks may be performed at the level of PROTECTED A / B (as required) including an IT Link at the level of PROTECTED A / B (as required).

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

The Contractor/Offeror must comply with the provisions of the:

c) Security Requirements Check List and security guide (if applicable), attached at Annex B and C;
d) Contract Security Manual (Latest Edition);
e) CSP website: Security requirements for contracting with the Government of Canada, located at https://www.tpsgc-pwgsc.gc.ca/esc-src/index-eng.html

33 Industrial Security Program – Security Requirements for Foreign Suppliers

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

a) The **Contractor/Subcontractor** certifies that the delivery and provisioning of Cloud Services under the terms of this contract must be from a country within the North Atlantic Treaty Organization (NATO), the European Union (EU) or from a country with which Canada has an international bilateral security instrument. The Contract Security Program (CSP) has international bilateral security instruments with the countries listed on the following PSPC website: http://www.tpsgc-pwgsc.gc.ca/esc-src/international-eng.html and as updated from time to time.

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

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

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

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

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

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

i. not be disclosed to another government, person or firm, or representative thereof not directly related to the performance of the **contract**, without the prior written consent of Canada. Such consent must be sought from the Canadian DSA in collaboration with the Contracting Authority; and
ii. not be used for any purpose other than for the performance of the **contract** without the prior written approval Canada. This approval must be obtained by contacting the Contracting Authority (in collaboration with the Canadian DSA).

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

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

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

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

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

The Foreign recipient Contractor requiring access to CANADA PROTECTED information/assets or Canadian restricted sites, under this contract, must submit a Request for Site Access to the Chief Security Officer of Name of Department/Organization of Canada.

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

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

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

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

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

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

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

Government of Canada / Gouvernement du Canada

PROTECTED B
When Filled

Supply Chain Security Information (SCSI)
Vendor Submission Form

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

PART B - PRODUCT LIST
CLICK HERE TO ADD ITEMS +

PART C - OWNERSHIP INFORMATION
CLICK HERE TO ADD ITEMS +

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

Revision 2019-06-19
CCCS# 9193325

Government of Canada / Gouvernement du Canada

PROTECTED B
When filled

B - Product List

Example IT Product List

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Supplier Name	Supplier DUNS Number	Supplier URL	Additional Information
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										
20										
21										
22										
23										
24										
25										
26										
27										
28										
29										
30										
31										
32										
33										
34										
35										
36										
37										
38										
39										
40										
41										

Government of Canada / Gouvernement du Canada

TLP AMBER
When Filled

C - Ownership Information

F - Example Owership Information

Use this form only for OEM and Suppliers that do not have a DUNS number.

Item	OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						

D - Help

Field	Guide	Notes
SCSI Form 2 Cover		
PROCUREMENT NAME	If not applicable, leave blank. Otherwise, provide any name associated with this multi-line procurement (i.e. WTD Print, Project Telesto).	
Date submitted:	YYYY-MM-DD	
SOLICITATION #:	If not applicable, leave blank. Otherwise, provide the solicitation number for this multi-line procurement.	
BIDDER NAME	If not applicable, leave blank. Enter the name of the lead organization providing the bid submission.	
BIDDER DUNS Number	If not applicable, leave blank. Enter the DUNS number of the lead organization providing the bid submission. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.	
IT PRODUCT LIST		
OEM Name	Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered.	**Only products that qualify for supply chain integrity assessments should be included in this list. Power cables, rack blanking panels, warranty costs, shipping costs, and similar other non-ICT items should not be included. If these products are found in this form, it will be sent back as incorrect and no assessment will be performed.**
OEM DUNS Number	Enter the DUNS number of the OEM. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a business. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question.	
Product Name	Enter the OEM's name for the product.	
Model Number	Enter the OEM's model and/or version number of the product.	
Product URL	Enter the URL of the OEM's webpage for the product.	

Vulnerability Information	Enter information concerning the last 5 security issues that were reported about the product. If the OEM posts this information to the CVE website, list the CVE numbers **separated by semi-colons (;)**. If the OEM does not post this information to the CVE website, you will need to ask the OEM directly for security vulnerability information and provide this information to the Canadian Centre for Cyber Security. If this is the case for a particular product, enter "see attached information" in the relevant field(s).	**This should follow the "Product" definition of "hardware (or software) that operates at the data link layer of the Open Systems Interconnection model (OSI Model) Layer 2 and above"**
Supplier Name	Enter the name of the supplier (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product that is being ordered. This includes any business entity involved in producing products or services to help complete the bidding requirements. **For PISA, NMSO, or similar lists, this field may be left blank.**	
Supplier DUNS Number	Enter the DUNS number of the Supplier. The Data Universal Numbering System (DUNS) is a unique nine-digit number assigned to each physical location of a businesses. It is a worldwide standard and is used to determine the credit score of a company. If the company does not have a DUNS number, or you are unable to find one, please fill out the requested information on "C - Ownership Information". Ownership information consists of the top 5, by percentage, investors and owners of the company. The names provided for investors and owners should be those found in investment or ownership documents for the company in question. **For PISA, NMSO, or similar lists, this field may be left blank.**	
Supplier URL	Enter the URL of the supplier's webpage for the product. **For PISA, NMSO, or similar lists, this field may be left blank.**	
OWNERSHIP INFORMATION		
OEM or Supplier name	Enter the name of the original equipment manufacturer (OEM) of the product that is being ordered, or enter the name of the supplier (i.e. sub-contractors, re-seller, distributor, sub-processors, etc.) of the product or service that is being ordered.	**It is only necessary to fill out entries in "C- Ownership Information" if a DUNS number cannot be supplied for the OEM and/or supplier.** **Each piece of provided information must be found on its own line in its own cell in the spreadsheet.**
Ownership	Ownership information consists of the top 5, by percentage, owners of the OEM or Supplier. The names provided for owners should be those found in ownership documents for the company in question.	
Investors	Investor information consists of the top 5, by percentage, investor in the OEM or Supplier. The names provided for owners should be those found in investment documents for the company in question.	
Executives	List the executives and members of the board of directors for the company in question.	
Country / Nationality	The country which an individual listed has their primary nationality or the country in which a corporate entity is registered.	
Corporate website link	For each of OEM or Supplier name, Ownership, Investors, and Executives listed above provide a URI / URL to the information that supports the claims listed in each of the fields.	

E - Example IT Product List

Item	OEM Name	OEM DUNS Number	Product Name	Model / Version	Product URL	Vulnerability Information	Supplier Name	Supplier DUNS Number	Supplier URL	ADDITIONAL INFORMATION
1	Cisco	137660665	1941	K9	https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW				PISA Example
2	Cisco	137660665	1941	K9	https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html	CVE-2018-XXXXX; CVE-2018-YYYYY; CVE-2018-XXXXX; CVE-2017-WWWWW	LocalHardware	4567891234	https://www.lhinc.ca	ROC / Single Procurement Example

F - Example Owership Information

OEM or Supplier name	Ownership	Investors	Executives	Country / Nationality	Corporate website link
newkid software	Mr. A (60%)			Canada	newkid.com/profiles/mra
newkid software	Ms. B (30 %)			France	newkid.com/profiles/msb
newkid software	Mr. C (10%)			United States	newkid.com/profiles/mrc
newkid software		Company A (10%)		United States	newkid.com/investor_relations/filings
newkid software		Company B (9%)		China	newkid.com/investor_relations/filings
newkid software		Company C (8%)		South Korea	newkid.com/investor_relations/filings
newkid software		Company D (5%)		Canada	newkid.com/investor_relations/filings
newkid software		Company E (5%)		Spain	newkid.com/investor_relations/filings
newkid software			Mr. A	Canada	newkid.com/profiles/mra
newkid software			Ms. B	France	newkid.com/profiles/msb
newkid software			Mr. Q	Portugal	newkid.com/profiles/mrq

Shared Services Canada

DRAFT

Conferencing & Operator Assisted Service (COAS)

Appendix 1 of Annexes A, B & C - Glossary

Version 1.0

Table of Contents

1 GLOSSARY OF TERMS

Term or Acronym	Definition
Accessible Canada Act	An Act legislated by the Federal Government of Canada to ensure a barrier free Canada Accessible Canada Act (justice.gc.ca)
American Sign Language	American Sign Language (ASL) is a complete, natural language that has the same linguistic properties as spoken languages, with grammar that differs from English. ASL is expressed by movements of the hands and face. It is the primary language of many North Americans who are deaf and hard of hearing and is used by some hearing people as well.
Audio Conference	A conference in which participants in different locations connect via telephone or Internet connections to interactively communicate with each other in real time.
Audio Conference Recording	Audio Conference Recording means any recording made by any electronic device capable of recording sound. This includes but is not limited to recordings made by digital audio files and stored on a computer, or in any other format.
Billing Code	A numeric code created and used by Government departments for cataloguing information related for financial or reporting purposes.
Breakout Rooms	Breakout rooms are sessions that are split off from the main conference. They allow the participants to meet in smaller groups and are completely isolated in terms of audio and video from the main session. Breakout rooms can be used for collaboration and discussion of the conference.
Change Management	Change Management is the process of tracking and managing a change throughout its entire life cycle, from start to closure, with the aim to minimize risk.
Department Code	A Code that defines the different Government departments. Department Codes determine which general ledger income accounts are affected by transactions.
Dial Out	The Operator or Moderator of the conference calls out to one or more people for the purpose of connecting them to the conference.
Full Duplex	A duplex communication system is a point-to-point system composed of two or more connected parties or devices that can communicate with one another in both directions.
Host or Co-Host	A Host or Co-Host is a person(s) who presides over an audio/web, webcast or operator assisted conference.
Incident	An Incident can be defined as an unanticipated or unplanned interruption in the delivery of IT service or a significant reduction in the quality of an IT service.
Incident Management	Incident Management is the process used by operations teams to respond to an unplanned event or service interruption and restore the service to its operational state.
Incident Tickets	An Incident Ticket is the documentation of an event or occurrence that details Incident(s) which governs and controls how an Incident Ticket is processed and routed between different resources for resolution.
In-Service Date	In-Service Date is the date on which the Contractor becomes solely and fully responsible for providing the COAS.
Locked Access	Locking a meeting stops anyone, including invitees, from joining the meeting.
Official Languages Act	The Official Languages Act is the federal statute that made English and French the official languages of Canada. It requires all federal institutions to provide services spoken in both Official Languages of Canada (English or French) on request.
Operator	The Contractor's primary person who performs activities during conferences, such as but not limited to, tests the audio and web, connecting and greeting all Participants into a conference, provide instructions, introduces speakers, manages Q&A and polling and first-level audio and web issues.

Operational Readiness	Operational Readiness is a state that is moved toward incrementally by performing tasks and creating deliverables throughout the project lifecycle.
Participant(s)	An individual (or group of individuals) participating in a conference session that may or may not be a GC employee or a Subscriber.
Partner	Those government institutions for which SSC services are mandatory for IT-infrastructure services related to email, data centres and telecommunications. Click here for the list of Partners. https://service.ssc-spc.gc.ca/en/aboutus/partner-clients
Presenter	A person responsible for presenting any presentation information to Participants during a conferencing event.
Problem	A Problem is a cause or potential cause of one or more incidents.
Problem Ticket	Problem Ticket is a document in electronic form that is in the Problem tracking system to record a Problem Call and track the resolution of the Problem.
Role-Based Access Control (RBAC)	Role-based access control (RBAC) is a policy-neutral access-control mechanism defined around roles and privileges and as such, is a method of restricting user access to Information System based on specified roles. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments.
Security Assessment and Authorization (SA&A)	The process by which Canada examines and develops the security evidence of Information Systems and Services for issuance of Authority to Operate that is necessary for achieving In-Service.
Service Desk	The Contractor's single point of contact between themselves and Canada to manage the COAS Service providing the Users the ability to report Incidents and service requests as well as handling communications on a day-to-day basis.
Subscriber	The Subscriber is an individual or a group of individuals each with a Portal Account identified to the system by a Username and Password.
Uniform Resource Locator (URL)	String of characters defined per IETF RFC 3986 that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. An example of a typical URL would be "http://en.example.org ".
User Profile	A User Profile is *a collection of settings and information associated with a user*. It contains critical information that is used to identify an individual.
User	A User is a person listed or identified who is authorized to have a Service Portal Account and access any of the COAS Services.

This Appendix contains a mocked up EBDF file to aid the Contractor in understanding the file requirements. The Bidder is encouraged to understand cells that contain calculations to aid in understanding the file requirements for ingesting into Canada systems.

The EBDF will be read by SSC internal billing validation systems and must be in a CSV format.

The data in this sample is representative test data only to highlight the various billing line items, column headers, and field syntax and format as well as some foundational data.

Data, calculations, syntax and fields are only representational ion the mock up to aid in creation of the Contractor's final file format which must be provided in the SRS.

Record Type	Invoice Date	Invoice Period	Canada Contract Identifier	Contractor	Total Recurring Charges for the Month	Total Non-Recurring Charges for the Month	Total Usage Charges	Total Charges Excluding Taxes	Total Other Charges and Credits	Total Service Credits	Total Late Payment Amount	Total GST Amount	Total HST Amount	Total QST Amount	Total Taxes	Total Amount Including Taxes
1	20211001	202109	2B0KBGCNT3	Contractor Company Name	0.00	194849.00	3732.53	198581.53	-1078.00	-247000.00	0.00	58.15	25191.94	39.36	25289.45	-24207.02

Record Type	Row Number	Contractor Billing Account Number	Invoice Number	Invoice Period	SSC Reference Number	SSC Version	SSC Seq No	Department Code	Department	Taxable Prov	Billing Start Date	Billing End Date	SCID	SCID Description	Qty	Recurring Charges	Total Recurring Charges	Non-recurring Charges	Total Non-recurring Charges for the Month	Total Service Credits	Total Other Charges and Credits	Total GST Amount	Total HST Amount	Total QST Amount	Total Taxes	Total Amount including taxes
2	1	1234567890	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	AWAPPE	Audio Web Annual License cost per Active User:	10000.00			1.23	12300.00				1599.00		1599.00	13899.00
2	2	1234567891	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	AWRTTE	Real time translation (RTT) in both English and French	2000.00			2.34	4680.00				608.40		608.40	5288.40
2	3	1234567892	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	SPG1	Service Portal Design Build Gate 1	1.00			56123.00	56123.00				7295.99		7295.99	63418.99
2	4	1234567893	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	SPG2	Service Portal Design Build Gate 2	1.00			56123.00	56123.00				7295.99		7295.99	63418.99
2	5	1234567894	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	SPG3	Service Portal Design Build Gate 3	1.00			56123.00	56123.00				7295.99		7295.99	63418.99
2	6	1234567895	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	SPCRExxx	Feature Change (max price per full release cycle)	3.00			2500.00	7500.00				975.00		975.00	8475.00
2	7	1234567896	2377918	202109	102813	2	7	163	SSC	ON	2022114	2022114	SPSCExxx	Standard Change	2.00			1000.00	2000.00				260.00		260.00	2260.00
2	8	1234567897	2377918	202109	SLA credit note 123	2	7	163	SSC	ON	2022114	2022114	SLT-MTTR-COAS	Service Credit: Maximum Time to Restore the COAS 1st occurrence	4.00			5000.00		-20000.00					0.00	-20000.00
2	9	1234567897	2377918	202109	SLA credit note 124	2	7	163	SSC	ON	2022114	2022114	SLT-MTTR-COAS	Service Credit: Maximum Time to Restore the COAS 2nd occurrence	4.00			10000.00		-40000.00					0.00	-40000.00
2	10	1234567897	2377918	202109	SLA credit note 125	2	7	163	SSC	ON	2022114	2022114	SLT-MTTR-COAS	Service Credit: Maximum Time to Restore the COAS 3rd occurrence	4.00			15000.00		-60000.00					0.00	-60000.00
2	11	1234567897	2377918	202109	SLA credit note 126	2	7	163	SSC	ON	2022114	2022114	SLT-MTTR-COAS	Service Credit: Maximum Time to Restore the COAS additional 30 mins	4.00			1000.00		-4000.00					0.00	-4000.00
2	12	1234567898	2377918	202109	SLA credit note 127	2	7	163	SSC	ON	2022114	2022114	SLT-MTTR-SP	Service Credit: Maximum Time to Restore the Service Portal	1.00			10000.00		-10000.00					0.00	-10000.00
2	13	1234567898	2377918	202109	SLA credit note 128	2	7	163	SSC	ON	2022114	2022114	SLT-MTTR-SP	Service Credit: Maximum Time to Restore the Service Portal additional 30mins	5.00			1000.00		-5000.00					0.00	-5000.00
2	14	1234567899	2377918	202109	SLA credit note 129	2	7	163	SSC	ON	2022114	2022114	SLT-BA	Service Credit: Detailed Billing file accuracy, timing and format	6.00			1000.00		-6000.00					0.00	-6000.00
2	15	1234567900	2377918	202109	SLA credit note 130	2	7	163	SSC	ON	2022114	2022114	SLT-CONRES	Service Credit: Contractor Failure to Perform it's Responsibilities	7.00			1000.00		-7000.00					0.00	-7000.00
2	16	1234567901	2377918	202109	SLA credit note 131	2	7	163	SSC	ON	2022114	2022114	SLT-OR	Service Credit: Operational Readiness - SA&A Gate one time	1.00			20000.00		-20000.00					0.00	-20000.00
2	17	1234567901	2377918	202109	SLA credit note 132	2	7	163	SSC	ON	2022114	2022114	SLT-OR	Service Credit: Operational Readiness - SA&A Gate ongoing	5.00			2000.00		-10000.00					0.00	-10000.00
2	18	1234567901	2377918	202109	SLA credit note 133	2	7	163	SSC	ON	2022114	2022114	SLT-OR	Service Credit: Operational Readiness - Service Portal Gate one time	1.00			30000.00		-30000.00					0.00	-30000.00
2	19	1234567901	2377918	202109	SLA credit note 134	2	7	163	SSC	ON	2022114	2022114	SLT-OR	Service Credit: Operational Readiness - Service Portal Gate daily credit	5.00			2000.00		-10000.00					0.00	-10000.00
2	20	1234567901	2377918	202109	SLA credit note 135	2	7	163	SSC	ON	2022114	2022114	SLT-OR	Service Credit: Operational Readiness - COAS Services Gate ongoing	5.00			5000.00		-25000.00					0.00	-25000.00
2	21	1234567901	2377918	202109	Billing credit note 005	2	7	163	SSC	ON	2022114	2022114	BIL-CR	Billing OC&C Credit	1.00			2312.00			-2312.00		-300.56		-300.56	-2612.56
2	22	1234567901	2377918	202109	Billing debit note 001	2	7	163	SSC	ON	2022114	2022114	BIL-DB	Billing OC&C Debit	1.00			1234.00			1234.00		160.42		160.42	1394.42

Record Type	Row Number	Contractor Billing Account Number	Invoice Number	Period of Service	Department Code	Department	SCID	SCID Description	Port Start date / time	Port Disconnect date / time	quantity of port minutes	user identifier	conference identifier	Subscribers ID	date and time of rescheduling or cancelling	SR requested date and time	scheduled start time	User Name	Telephone Number	Call Type	Conference Title	Number of Operators reserved	Number of Actual Operators	reserved ports	actual ports	unused ports	Usage Charge	Total Usage Charges for the Month	tax province	Total GST Amount	Total HST Amount	Total QST Amount	Total Taxes	Total Amount including taxes
3	1	aaabbbccc1	INV#123	01-2022	34	TC	OASCY01	OAS Price per minute per active port FGWD - Year 1	20220101 00:00:00	20220101 00:10:00	100	first.last@TC.gc.ca	abc123-01	abc123-01		20211225 00:00:00	20220101 00:00:00	first.last@canada.ca	(123)456-7890		Meeting Title 1	1	1				1.00	100.00	NL		0.15		0.15	100.15
3	2	aaabbbccc2	INV#123	01-2022	35	NRC	OASCY02	OAS Price per minute per active port FGWD - Year 2	20220102 00:00:00	20220102 00:11:00	101	first.last@NRC.gc.ca	abc123-02	abc123-02		20211226 00:00:00	20220102 00:00:00	first.last@canada.ca	(123)456-7891		Meeting Title 2	2	2				1.05	106.05	PE		0.15		0.15	106.20
3	3	aaabbbccc3	INV#123	01-2022	53	CSC	OASCY03	OAS Price per minute per active port FGWD - Year 3	20220103 00:00:00	20220103 00:12:00	102	first.last@CSC.gc.ca	abc123-03	abc123-03		20211227 00:00:00	20220103 00:00:00	first.last@canada.ca	(123)456-7892		Meeting Title 3	3	3				1.10	112.46	NS		0.05		0.05	112.51
3	4	aaabbbccc4	INV#123	01-2022	37	TELECAN	OASCY04	OAS Price per minute per active port FGWD - Year 4	20220104 00:00:00	20220104 00:10:31	103	first.last@TELECAN.gc.ca	abc123-04	abc123-04		20211228 00:00:00	20220104 00:00:00	first.last@canada.ca	(123)456-7893		Meeting Title 4	4	4				1.16	119.24	NB		0.15		0.15	119.39
3	5	aaabbbccc5	INV#123	01-2022	54	StatsCan	OASCY05	OAS Price per minute per active port FGWD - Option Year 5	20220105 00:00:00	20220105 00:10:00	104	first.last@StatsCan.gc.ca	abc123-05	abc123-05		20211229 00:00:00	20220105 00:00:00	first.last@canada.ca	(123)456-7894		Meeting Title 5	5	5				1.22	126.41	QC	6.32		12.61	18.93	145.34
3	6	aaabbbccc6	INV#123	01-2022	39	NFB	OASCY06	OAS Price per minute per active port FGWD - Option Year 6	20220106 00:00:00	20220106 00:10:00	105	first.last@NFB.gc.ca	abc123-06	abc123-06		20211230 00:00:00	20220106 00:00:00	first.last@canada.ca	(123)456-7895		Meeting Title 6	6	6				1.28	134.01	ON		0.13		0.13	134.14
3	7	aaabbbccc7	INV#123	01-2022	40	CTA	OASCY07	OAS Price per minute per active port FGWD - Option Year 7	20220107 00:00:00	20220107 00:10:00	106	first.last@CTA.gc.ca	abc123-07	abc123-07		20211231 00:00:00	20220107 00:00:00	first.last@canada.ca	(123)456-7896		Meeting Title 7	7	7				1.34	142.05	MB	7.10			7.10	
3	8	aaabbbccc8	INV#123	01-2022	41	NRCan	OASCY08	OAS Price per minute per active port FGWD - Option Year 8	20220108 00:00:00	20220108 00:10:00	107	first.last@NRCan.gc.ca	abc123-08	abc123-08		20220101 00:00:00	20220108 00:00:00	first.last@canada.ca	(123)456-7897		Meeting Title 8	8	8				1.41	150.56	SK	7.53			7.53	
3	9	aaabbbccc9	INV#123	01-2022	42	CIRNAC	OASCY09	OAS Price per minute per active port FGWD - Option Year 9	20220109 00:00:00	20220109 00:10:00	108	first.last@CIRNAC.gc.ca	abc123-09	abc123-09		20220102 00:00:00	20220109 00:00:00	first.last@canada.ca	(123)456-7898		Meeting Title 9	9	9				1.48	159.57	AB		0.05		0.05	159.62
3	10	aaabbbccc10	INV#123	01-2022	43	CICS	OASCY10	OAS Price per minute per active port FGWD - Option Year 10	20220110 00:00:00	20220110 00:10:00	109	first.last@CICS.gc.ca	abc123-10	abc123-10		20220103 00:00:00	20220110 00:00:00	first.last@canada.ca	(123)456-7899		Meeting Title 10	10	10				1.55	169.09	BC	8.45			8.45	
3	11	aaabbbccc11	INV#123	01-2022	44	WD	OASNY01	OAS Price per minute per active port non-FGWD - Year 1	20220111 00:00:00	20220111 00:10:00	110	first.last@WD.gc.ca	abc123-11	abc123-11		20220104 00:00:00	20220111 00:00:00	first.last@canada.ca	(123)456-7900		Meeting Title 11	11	11				1.63	179.18	NU		0.05		0.05	179.23
3	12	aaabbbccc12	INV#123	01-2022	56	TBS	OASNY02	OAS Price per minute per active port non-FGWD - Year 2	20220112 00:00:00	20220112 00:10:00	111	first.last@TBS.gc.ca	abc123-12	abc123-12		20220105 00:00:00	20220112 00:00:00	first.last@canada.ca	(123)456-7901		Meeting Title 12	12	12				1.71	189.85	NT		0.15		0.15	190.00
3	13	aaabbbccc13	INV#123	01-2022	46	PSIC	OASNY03	OAS Price per minute per active port non-FGWD - Year 3	20220113 00:00:00	20220113 00:10:00	112	first.last@PSIC.gc.ca	abc123-13	abc123-13		20220106 00:00:00	20220113 00:00:00	first.last@canada.ca	(123)456-7902		Meeting Title 13	13	13				1.80	201.14	YT		0.05		0.05	201.19
3	14	aaabbbccc14	INV#123	01-2022	47	CNSC	OASNY04	OAS Price per minute per active port non-FGWD - Year 4	20220114 00:00:00	20220114 00:10:00	113	first.last@CNSC.gc.ca	abc123-14	abc123-14		20220107 00:00:00	20220114 00:00:00	first.last@canada.ca	(123)456-7903		Meeting Title 14	14	14				1.89	213.08	NL		0.15		0.15	213.23
3	15	aaabbbccc15	INV#123	01-2022	57	PBC	OASNY05	OAS Price per minute per active port non-FGWD - Option Year 5	20220115 00:00:00	20220115 00:10:00	114	first.last@PBC.gc.ca	abc123-15	abc123-15		20220108 00:00:00	20220115 00:00:00	first.last@canada.ca	(123)456-7904		Meeting Title 15	15	15				1.98	225.71	PE		0.15		0.15	225.86
3	16	aaabbbccc16	INV#123	01-2022	53	CSC	OASNY06	OAS Price per minute per active port non-FGWD - Option Year 6	20220116 00:00:00	20220116 00:10:00	115	first.last@CSC.gc.ca	abc123-16	abc123-16		20220109 00:00:00	20220116 00:00:00	first.last@canada.ca	(123)456-7905		Meeting Title 16	16	16				2.08	239.08	NS		0.05		0.05	239.13
3	17	aaabbbccc17	INV#123	01-2022	50	IRCC	OASNY07	OAS Price per minute per active port non-FGWD - Option Year 7	20220117 00:00:00	20220117 00:10:00	116	first.last@IRCC.gc.ca	abc123-17	abc123-17		20220110 00:00:00	20220117 00:00:00	first.last@canada.ca	(123)456-7906		Meeting Title 17	17	17				2.18	253.21	NB		0.15		0.15	253.36
3	18	aaabbbccc18	INV#123	01-2022	51	FJA	OASNY08	OAS Price per minute per active port non-FGWD - Option Year 8	20220118 00:00:00	20220118 00:10:00	117	first.last@FJA.gc.ca	abc123-18	abc123-18		20220111 00:00:00	20220118 00:00:00	first.last@canada.ca	(123)456-7907		Meeting Title 18	18	18				2.29	268.17	QC	13.41		26.75	40.16	
3	19	aaabbbccc19	INV#123	01-2022	52	CSPS	OASNY09	OAS Price per minute per active port non-FGWD - Option Year 9	20220119 00:00:00	20220119 00:10:00	118	first.last@CSPS.gc.ca	abc123-19	abc123-19		20220112 00:00:00	20220119 00:00:00	first.last@canada.ca	(123)456-7908		Meeting Title 19	19	19				2.41	283.98	ON		0.13		0.13	284.11
3	20	aaabbbccc20	INV#123	01-2022	53	CSC	OASNY10	OAS Price per minute per active port non-FGWD - Option Year 10	20220120 00:00:00	20220120 00:10:00	119	first.last@CSC.gc.ca	abc123-20	abc123-20		20220113 00:00:00	20220120 00:00:00	first.last@canada.ca	(123)456-7909		Meeting Title 20	20	20				2.53	300.71	MB	15.04			15.04	
3	21	aaabbbccc21	INV#123	01-2022	54	StatCan	OASCRNE	Cancellation or Reschedule Fees < 24 hours (Flat fee per conference)	20220121 00:00:00	20220121 00:10:00		first.last@StatCan.gc.ca	abc123-21	abc123-21	20220121 00:00:00	20220121 00:10:00	20220121 00:10:00	first.last@canada.ca	(123)456-7910		Meeting Title 21	21	21				2.00	2.00	SK	0.10			0.10	
3	22	aaabbbccc22	INV#123	01-2022	57	PBC	OASEMCE	Emergency Conference Type 1 Premium (scheduled < 30 minutes before start)	20220122 00:00:00	20220122 00:10:00		first.last@PBC.gc.ca	abc123-22	abc123-22	20220122 00:00:00	20220122 00:10:00	20220122 00:10:00	first.last@canada.ca	(123)456-7911		Meeting Title 22	22	22				3.00	3.00	AB		0.05		0.05	3.05
3	23	aaabbbccc23	INV#123	01-2022	56	TBS	OASEMEE	Emergency Conference Type 2 Premium (scheduled >30 minutes but less than 120 minutes)	20220123 00:00:00	20220123 00:10:00		first.last@TBS.gc.ca	abc123-23	abc123-23	20220123 00:00:00	20220123 00:10:00	20220123 00:10:00	first.last@canada.ca	(123)456-7912		Meeting Title 23	23	23				4.00	4.00	BC	0.20			0.20	
3	24	aaabbbccc24	INV#123	01-2022	61	CIHR	OASUNPE	Unused port Fees >10% (Flat fee per port)	20220124 00:00:00	20220124 00:10:00		first.last@CIHR.gc.ca	abc123-24	abc123-24	20220124 00:00:00	20220124 00:10:00	20220124 00:10:00	first.last@canada.ca	(123)456-7913		Meeting Title 24	24	24	33	32	1	0.00	0.00	NU		0.05		0.05	0.05
3	25	aaabbbccc24	INV#123	01-2022	61	CIHR	OASUNPE	Unused port Fees >10% (Flat fee per port)	20220124 00:00:00	20220124 00:10:00		first.last@CIHR.gc.ca	abc123-24	abc123-24	20220124 00:00:00	20220124 00:10:00	20220124 00:10:00	first.last@canada.ca	(123)456-7914		Meeting Title 25	25	25	100	50	50	1.00	50.00	NU		0.05		0.05	50.05

DRAFT

deptID	deptLegalTitleEn	deptLegalTitleFr	deptAppliedNameEn	deptAppliedNameFr	deptAccEn	deptAccFr	deptSSCPartner	deptSSCClient
1	Department of Agriculture and Agri-Food	Ministère de l'Agriculture et de l'Agroalimentaire	Agriculture an	Agriculture et	AAFC	AAC	1	0
2	Office of the Auditor General	Bureau du vérificateur général	Office of the A	Bureau du vér	OAG	BVG	0	1
4	Public Service Commission	Commission de la fonction publique	Public Service	Commfission	PSC	CFP	1	0
5	Department of Foreign Affairs, Trade and Development	Ministère des Affaires étrangères, du Commerce et du De	Global Affairs	Affaires mond	GAC	AMC	1	0
6	Department of Finance	Ministère des Finances	Department o	Ministère des	FIN	FIN	1	0
7	Department of the Environment	Ministère de l'Environnement	Environment a	Environnemer	ECCC	ECCC	1	0
8	Office of the Governor General's Secretary	Bureau du secrétaire du gouverneur général	Office of the S	Bureau du sec	OSGG	BSGG	0	1
9	Senate of Canada	Sénat du Canada	Senate	Sénat	SOC	SOC	0	1
11	Office of the Superintendent of Financial Institutions	Bureau du surintendant des institutions financières	Office of the S	Bureau du sur	OSFI	BSIF	0	1
12	Economic Development Agency of Canada for the Regions of Quebec	Agence de développement économique du Canada pour	Canada Econ	Développeme	CED	DEC	1	0
13	Department of Justice	Ministère de la Justice	Department o	Ministère de la	JUS	JUS	1	0
14	Department of Employment and Social Development	Ministère de l'Emploi et du Développement social	Employment a	Emploi et Dév	ESDC	EDSC	1	0
15	Office of the Chief Electoral Officer	Bureau du directeur général des élections	Elections Can	Élections Can	elections	elections	0	1
16	Canadian Radio-television and Telecommunications Commission	Conseil de la radiodiffusion et des télécommunications ca	Canadian Rad	Conseil de la	CRTC	CRTC	0	0
17	Library of Parliament	Bibliothèque du Parlement					0	0
18	Department of National Defence	Ministère de la Défense nationale	National Defe	Défense natio	DND	MDN	1	0
19	Office of the Director of Public Prosecutions	Bureau du directeur des poursuites pénales	Public Prosec	Service des p	PPSC	SPPC	0	1
21	Department of Veterans Affairs	Ministère des Anciens Combattants	Veterans Affa	Anciens Com	VAC	ACC	1	0
22	Department of Health	Ministère de la Santé	Health Canad	Santé Canada	HC	SC	1	0
23	Atlantic Canada Opportunities Agency	Agence de promotion économique du Canada atlantique			ACOA	APECA	1	0
24	International Joint Commission (Canadian Section)	Commission mixte internationale (section canadienne)					0	0
25	Privy Council Office	Bureau du Conseil privé	Privy Council	Bureau du Co	PCO	BCP	1	0
27	Natural Sciences and Engineering Research Council	Conseil de recherches en sciences naturelles et en génie	Natural Scien	Conseil de rec	NSERC	CRSNG	0	1
30	Royal Canadian Mounted Police	Gendarmerie royale du Canada			RCMP	GRC	1	0
32	Immigration and Refugee Board	Commission de l'immigration et du statut de réfugié	Immigration a	Commission d	IRB	CISR	1	0
33	Department of Industry	Ministère de l'Industrie	Innovation, Sc	Innovation, Sc	ISED	ISDE	1	0
34	Department of Transport	Ministère des Transports	Transport Can	Transports Ca	TC	TC	1	0
35	National Research Council of Canada	Conseil national de recherches du Canada	National Rese	Conseil nation	NRC	CNRC	1	0
37	Telefilm Canada	Téléfilm Canada			TELECAN	TELECAN	0	1
38	Canada Border Services Agency (Administered Activities)	Agence des services frontaliers du Canada (activités administrées)					0	0
39	National Film Board	Office national du film			NFB	ONF	0	0
40	Canadian Transportation Agency	Office des transports du Canada	Canadian Tra	Office des tra	CTA	OTC	0	0
41	Department of Natural Resources	Ministère des Ressources naturelles	Natural Resou	Ressources n	NRCan	RNCan	1	0
42	Department of Crown-Indigenous Relations and Northern Affairs	Ministère des Relations Couronne-Autochtones et des Aff	Crown-Indiger	Relations Cou	CIRNAC	RCAANC	1	0
43	Canadian Intergovernmental Conference Secretariat	Secrétariat des conférences intergouvernementales canadiennes			CICS	SCIC	0	1
44	Department of Western Economic Diversification	Ministère de la Diversification de l'économie de l'Ouest ca	Western Econ	Diversification	WD	DEO	1	0
46	Office of the Public Sector Integrity Commissioner	Commissariat à l'intégrité du secteur public	Office of the F	Commissariat	PSIC	ISPC	0	1
47	Canadian Nuclear Safety Commission	Commission canadienne de sûreté nucléaire	Canadian Nuc	Commission d	CNSC	CCSN	1	0
50	Department of Citizenship and Immigration	Ministère de la Citoyenneté et de l'Immigration	Immigration, R	Immigration, R	IRCC	IRCC	1	0
51	Office of the Commissioner for Federal Judicial Affairs	Bureau du commissaire à la magistrature fédérale	Office of the C	Commissariat	FJA	CMF	0	1
52	Canada School of Public Service	École de la fonction publique du Canada			CSPS	EFPC	1	0
53	Correctional Service of Canada	Service correctionnel du Canada	Correctional S	Service correc	CSC	SCC	1	0
54	Statistics Canada	Statistique Canada	Statistics Can	Statistique Ca	StatCan	StatCan	1	0
56	Treasury Board Secretariat	Secrétariat du Conseil du Trésor	Treasury Boar	Secrétariat du	TBS	SCT	1	0
57	Parole Board of Canada	Financement agricole Canada	Parole Board	Commission d	PBC	CLCC	0	1
61	Canadian Institutes of Health Research	Instituts de recherche en santé du Canada			CIHR	IRSC	0	1

deptID	deptLegalTitleEn	deptLegalTitleFr	deptAppliedNameEn	deptAppliedNameFr	deptAccEn	deptAccFr	deptSSCPartner	deptSSCClient
62	Federal Economic Development Agency for Southern Ontario	Agence fédérale de développement économique pour le	Federal Econ	Agence fédéra	FedDev Ontar	FedDev Ontario	1	0
63	Social Sciences and Humanities Research Council	Conseil de recherches en sciences humaines	Social Scienc	Conseil de rec	SSHRC	CRSH	0	0
66	Northern Pipeline Agency	Administration du pipe--line du Nord	Northern Pipe	Administration	NPA	APN	0	0
67	House of Commons	Chambres des communes			HoC	CdC	0	1
75	Canadian Human Rights Commission	Commission canadienne des droits de la personne			CHRC	CCDP	0	1
76	Office of the Commissioner of Official Languages	Commissariat aux langues officielles			OCOL	CLO	0	0
78	Canadian Northern Economic Development Agency	Agence canadienne de développement économique du N	Canadian Nor	Agence canad	CanNor	CanNor	1	0
79	Payroll System General Ledger	Grand livre général du système de la paye					0	0
80	Registrar of the Supreme Court of Canada and that portion of the federal public admin	Registraire de la Cour suprême du Canada et le secteur d	Registrar of th	Registraire de	SCC	CSC	0	1
85	Canada Border Services Agency	Agence des services frontaliers du Canada	Canada Borde	Agence des s	CBSA	ASFC	1	0
86	Department of Fisheries and Oceans	Ministère des Pêches et des Océans	Fisheries and	Pêches et Oc	DFO	MPO	1	0
87	Public Service Superannuation	Pension de retraite de la fonction publique					0	0
88	Department of Public Safety and Emergency Preparedness	Ministère de la Sécurité publique et de la Protection civile	Public Safety	Sécurité publi	PS	SP	1	0
91	Canada Mortgage and Housing Corporation	Société canadienne d'hypothèques et de logement	Canada Mortg	Société canad	CMHC	SCHL	0	1
95	Canadian Security Intelligence Service	Service canadien du renseignement de sécurité	Canadian Sec	Service canad	CSIS	SCRS	0	1
96	Offices of the Information and Privacy Commissioners of Canada	Commissariats à l'information et à la protection de la vie privée au Canada			OIC	CI	0	1
97	Receiver General	Receveur général					0	0
100	Canadian Centre for Occupational Health and Safety	Centre canadien d'hygiène et de sécurité au travail			CCFA	CADC	0	1
101	Canadian Transportation Accident Investigation and Safety Board	Bureau canadien d'enquête sur les accidents de transpor	Transportation	Bureau de la s	TSB	BST	0	1
102	The National Battlefields Commission	Commission des champs de bataille nationaux	The National I	Commission d	NBC	CCBN	0	0
103	National Security and Intelligence Review Agency Secretariat	Secrétariat de l'Office de surveillance des activités en ma	Security Intelli	Comité de sur	NSIRA	OSSNR	0	1
109	Patented Medicine Prices Review Board	Conseil d'examen du prix des médicaments brevetés	Patented Med	Conseil d'exa	PMPRB	CEPMB	0	1
116	Copyright Board	Commission du droit d'auteur	Copyright Boa	Commission d	CB	CDA	0	1
119	Canadian Space Agency	Agence spatiale canadienne	Canadian Spa	Agence spatia	CSA	ASC	1	0
122	Canada Revenue Agency (Administered Activities)	Agence du revenu du Canada (activités administrées)					0	0
123	Export Development Canada	Exportation et développement Canada	Export Develo	Exportation et	EDC	EDC	0	0
124	Parks Canada Agency	Agence Parcs Canada	Parks Canada	Parcs Canada	PC	PC	1	0
127	Department of Public Works and Government Services	Ministère des Travaux publics et des Services gouvernem	Public Service	Services publi	PSPC	SPAC	1	0
130	Canada Revenue Agency	Agence du revenu du Canada			CRA	ARC	1	0
133	Canadian Grain Commission	Commission canadienne des grains			CGC	CCG	0	0
134	Canadian Dairy Commission	Commission canadienne du lait	Canadian Dai	Commission d	CDC	CCL	0	1
135	Department of Canadian Heritage	Ministère du Patrimoine canadien	Canadian Her	Patrimoine ca	PCH	PCH	1	0
136	Canadian Food Inspection Agency	Agence canadienne d'inspection des aliments	Canadian Foo	Agence canad	CFIA	ACIA	1	0
137	Military Police Complaints Commission	Commission d'examen des plaintes concernant la police	Military Police	Commission d	MPCC	CPPM	0	1
138	Military Grievances External Review Committee	Comité externe d'examen des griefs militaires	Military Grieva	Comité extern	MGERC	CEEGM	0	1
139	Financial Transactions and Reports Analysis Centre of Canada	Centre d'analyse des opérations et déclarations financière	Financial Tran	Centre d'analy	FINTRAC	CANAFE	1	0
141	Financial Consumer Agency of Canada	Agence de la consommation en matière financière du Ca	Financial Con	Agence de la	FCAC	ACFC	0	1
142	Office of Infrastructure of Canada	Bureau de l'infrastructure du Canada	Infrastructure	Infrastructure	INFC	INFC	1	0
144	Courts Administration Service	Service administratif des tribunaux judiciaires	Courts Admin	Service admir	CAS	SATJ	0	0
145	Library and Archives of Canada	Bibliothèque et Archives du Canada	Library and Ar	Bibliothèque e	LAC	BAC	1	0
147	Office of the Conflict of Interest and Ethics Commissioner	Bureau du commissaire aux conflits d'intérêts et à l'éthique			CIEC	CCIE	0	1
148	Public Health Agency of Canada	Agence de la santé publique du Canada	Public Health	Agence de la	PHAC	ASPC	1	0
151	Office of the Senate Ethics Officer	Bureau du conseiller sénatorial en éthique					0	0
154	Office of the Commissioner of Lobbying	Commissariat au lobbying	Office of the C	Commissariat	OCL	CAL	0	0
163	Shared Services Canada	Services partagés Canada	Shared Servic	Services parta	SSC	SPC	1	0
165	Communications Security Establishment	Centre de la sécurité des télécommunications	Communicatio	Centre de la s	CSEC	CSTC	0	1

deptID	deptLegalTitleEn	deptLegalTitleFr	deptAppliedNameEn	deptAppliedNameFr	deptAccEn	deptAccFr	deptSSCPartner	deptSSCClient
170	Administrative Tribunals Support Service of Canada	Service canadien d'appui aux tribunaux administratifs	Administrative	Service canad	ATSSC	SCDATA	0	1
171	Canadian High Arctic Research Station	Station canadienne de recherche dans l'Extrême-Arctique	Polar Knowled	Savoir polaire	POLAR	POLAIRE	0	1
176	Parliamentary Protective Service	Service de protection parlementaire			PSS	SPP	0	1
180	Invest in Canada Hub	Investir au Canada					0	0
183	Office of the Parliamentary Budget Officer	Bureau du directeur parlementaire du budget					0	0
190	Department for Women and Gender Equality	Ministère des Femmes et de l'Égalité des genres	Women and G	Femmes et Ég	WAGE	FEGC	0	1
191	Department of Indigenous Services	Ministère des Services aux Autochtones	Indigenous Se	Services aux A	ISC	SAC	1	0
192	Secretariat of the National Security and Intelligence Committee of Parliamentarians	Secrétariat du Comité des parlementaires sur la sécurité	Secretariat of	Secrétariat du	SNSICP	SCPSNR	0	1
193	Leaders' Debates Commission	Commission des débats des chefs					0	0
195	Canadian Energy Regulator	Régie canadienne de l'énergie	Canada Energ	Régie de l'éne	CER	REC	0	0
197	Office of the Intelligence Commissioner	Bureau du commissaire au renseignement					0	0
199	Canadian Accessibility Standards Development Organization	Organisation canadienne d'élaboration de normes d'acce	Accessibility S	Normes d'acc	ASC	NAC	0	0
998	Test Department2	Test Department2	Test Departm	Test Departm	TST	TST	0	0
999	Test Department	Test Department	Test Departm	Test Departm	TEST	TEST	0	0
801001	Canadian Pari Mutual Agency	Agence canadienne du pari mutuel			CPMA	ACPM	0	1
801005	Canadian Commercial Corporation	Corporation commerciale canadienne	Canadian Cor	Corporation c	CCC	CCC	0	0
801006	Royal Canadian Mint	Monnaie royale canadienne			MINT	MONNAIE	0	1
801007	Impact Assessment Agency of Canada	Agence canadienne d'évaluation d'impact	Impact Assess	Agence d'éval	IACC	AEIC	0	1
801013	Supreme Court of Canada	Cours suprême du Canada			SCC	CSC	0	0
801018	Defence Research and Development Canada	Recherche et développement pour la Défense Canada			DRDC	RDDC	0	0
801025	Office of the Prime Minister	Cabinet du Premier Ministre			PMO	CMP	0	1
801033	Standards Council of Canada	Conseil canadien des normes			SCC	CCN	0	1
801034	Atlantic Pilotage Authority Canada	Administration de pilotage de l'Atlantique Canada	Atlantic Pilota	Administration	APA	APA	0	1
801041	Atomic Energy of Canada Limited	Énergie atomique du Canada, Limitée			AECL	EACL	0	1
801050	Passport Canada	Passport Canada			PPTC	PPTC	0	1
801053	Office of the Correctional Investigator of Canada	Bureau de l'enquêteur correctionnel du Canada	The Correctio	L'Enquêteur c	OCI	BEC	0	1
801086	Freshwater Fish Marketing Corporation	Office de commercialisation du poisson d'eau douce	Freshwater Fi	Office de com	FFMC	OCPED	0	1
801088	Civilian Review and Complaints Commission for the Royal Canadian Mounted Police	Commission civile d'examen et de traitement des plaintes	Civilian Revie	Commission c	CRCC	CCETP	0	1
801127	Canada Post Corporation	Société Postes Canada	Canada Post	Postes Canad	CPC	SCP	0	1
801130	Taxpayers' Ombudsman (Office of the)	Bureau de l'ombudsman des contribuables			OTO	BOC	0	1
801135	Canada Council for the Arts	Conseil des arts du Canada			BDC	BCD	0	1
801142	Windsor Detroit Bridge Authority	Authorité du pont Windsor Détroit	Windsor Detro	Autorité du po	WDBA	APWD	0	1
801165	Office of the Communications Security Establishment Commissioner	Bureau du Commissaire du Centre de la sécurité des télécommunications			OCSEC	BCCST0	0	1
802001	Farm Credit Canada	Financement Agricole Canada			FCC	FAC	0	1
802005	Business Development Bank of Canada	Banque de développement du Canada	Business Dev	Banque de dé	BDC	BDC	0	0
802006	Bank of Canada	Banque du Canada					0	0
802018	Defence Construction (1951) Limited	Construction de défense (1951) Limitée	Defence Cons	Construction d	DCC	CDC	0	0
802025	Democratic Institutions	Institutions démocratiques			DI	ID	0	1
802033	Canadian Tourism Commission	Commission canadienne du tourisme	Destination Ca	Destination Ca	DC	DC	0	1
802034	Canadian Air Transport Security Authority	Administration canadienne de la sureté du transport aérie	Canadian Air T	Administration	CATSA	ACSTA	0	1
802088	Royal Canadian Mounted Police External Review Committee	Comité externe d'examen de la Gendarmerie royale du C	RCMP Extern	Comité extern	ERC	CEE	0	1
802127	Office of Procurement Ombudsman	Bureau de l'ombudsman de l'approvisionnement			OPO	BOA	0	1
802135	Canadian Race Relations Foundation	Fondation canadienne des relations racial			CRRF	FCRR	0	1
803006	Canada Deposit Insurance Corporation	Société d'assurance-dépôts du Canada	Canada Depo	Société d'assu	CDIC	SADC	0	0
803025	Leader of the Government in the House of Commons	Leader du gouvernement à la Chambre des communes			LDHC	LGCC	0	1
803033	Communications Research Centre Canada	Centre de recherches sur les communications Canada			CRC	CRC	0	0

DRAFT

deptID	deptLegalTitleEn	deptLegalTitleFr	deptAppliedNameEn	deptAppliedNameFr	deptAccEn	deptAccFr	deptSSCPartner	deptSSCClient
803034	The Federal Bridge Corporation Limited	La Société des ponts fédéraux Limitée	Federal Bridg	Société des p	FBCL	SPFL	0	1
803127	Canada Lands Company Limited	Société immobilière du Canada Limitée			CLCL	SICL	0	0
803135	National Gallery of Canada	Musée des beaux-arts du Canada			NGC	MBAC	0	1
804034	Pacific Pilotage Authority Canada	Administration du pilotage du Pacifique Canada			PPA	APP	0	1
804127	National Capital Commission	Commission de la capitale nationale	National Capi	Commission d	NCC	CCN	0	0
804135	Canadian Museum for Human Rights	Musée canadien pour les droits de la personne			CMHR	MCDP	0	1
805034	Laurentian Pilotage Authority	Administration de pilotage de des Laurentides	Laurentian Pil	Administration	LPA	APL	0	0
805135	Canadian Museum of Nature	Musée canadien de la nature			CMN	MCN	0	1
806135	National Museum of Science and Technology	Musée national des sciences et de la technologie	Canada Scien	Musée des sc	CSTM	MSTC	0	0
807135	Canadian Conservation Institute	Institut canadien de conservation			CCI	ICC	0	0
808135	Canadian Museum of History	Musée canadien de l'histoire			CMH	MCH	0	1
809135	National Arts Centre	Centre National des Arts			NAC	CNA	0	0
701803127	Parc Downsview Park	Parc Downsview Park			PDP	PDP	0	0

Province / Territory Acronym	Province / Territory	Combined Rate	GST / HST	Provincial / Territorial Sales Tax
AB	Alberta	5.00%	5.00%	0
BC	British Columbia	12.00%	5.00%	7.00%
MB	Manitoba	12.00%	5.00%	7.00%
NB	New Brunswick	15.00%	15.00%	
NL	Newfoundland and Labrador	15.00%	15.00%	
NS	Northwest Territories	5.00%	5.00%	0
NT	Nova Scotia	15.00%	15.00%	
NU	Nunavut	5.00%	5.00%	0
ON	Ontario	13.00%	13.00%	
PE	Prince Edward Island	15.00%	15.00%	
QC	Quebec	14.98%	5.00%	9.98%
SK	Saskatchewan	11.00%	5.00%	6.00%
YT	Yukon	5.00%	5.00%	0

The Contractor must provide a printable Summary Invoiice in a non-modifyable format (e.g. pdf) which must, at a minimum, include the following:

1. Account Name
2. Contract Number
3. Account Name GOC - Shared Service Canada
4. Contract Number
5. Client Reference Number
6. Procurement Business Number
7. Statement Date
8. Account Number
9. Invoice Number
10. Invoice Due Date 30 days from acceptance
11. Invoice Period
12. Payments
13. Previous Rejected Amount
14. Subtotal
15. Total Monthly Charges
16. Total Non-Recurring Charges for the Month
17. Total Service Credits
18. GST
19. HST
20. QST
21. Total Taxes
22. Total Monthly Amount
23. Total Amount Due
24. GST/HST Registration#
25. QST Registration#
26. Contractor's Contact Information for Billing Questions
27. Contractor's Accounts Payable contact Information

Security Requirement ID	Security Requirement Sub-ID	Family	Name	Security Requirement	Related ITSG-33 Control
SR-1		AC	ACCOUNT MANAGEMENT	Roles and Permissions in the Service Portal must only be assigned by the DA role and the Contractor must ensure the following: a) establishing conditions for role membership; b) notify DA when: I) Accounts are no longer required; ii) users are terminated or transferred; iii) Service usage or need-to-know changes;	AC-2
SR-2		AC	ACCOUNT MANAGEMENT	Documents and folder permissions in the DMS must only be assigned by the TA role and the Contractor must ensure the following: a) establishing conditions for file and folder access; b) notify DA when: I) Permissions are no longer required; ii) users are terminated or transferred; iii) Service usage or need-to-know changes;	
SR-3		AC	ACCESS ENFORCEMENT	The Contractor must enforce approved authorizations for access to COAS Data and COAS System Components and restricting and minimize access only to Service Administrators with an explicit need to know access. COAS Services Administrators must use multi-factor authentication.	AC-3
SR-4		AC	ACCESS ENFORCEMENT	Service Portal accounts must ensure a domain filter is applied to account self-registration to only allow domains permitted by the TA.	AC-3
SR-5		AC	SEPARATION OF DUTIES	The Contractor must enforce separation of duties through Roles as defined in Annex A.	AC-5
SR-6	SR-6 (a)	AC	SYSTEM USE NOTIFICATION	The Audio Conferencing Service will present to Participants when joining an Audio Conference a message specified by Canada.	AC-8
	SR-6 (b)			The Web Conferencing Service will display to Participants when joining a Web Conference a message specified by Canada.	
SR-7	SR-7 (a)	AC	USE OF EXTERNAL INFORMATION SYSTEMS	If a third party or External Information System requires access to COAS Data, the Contractor must: a) establish terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining COAS Data; b) must only permit authorized individuals to use External Information System to access the COAS Data; c) Must provide to Canada the list of all COAS data that will be shared with third party or external information systems; and d) the Contractor must provide sufficient evidence that the third party or external information system adheres to Canada's Security Requirements. e) the Contractor must obtain Canada's approval for use of External Information Systems prior to any production data is shared with a third party.	AC-20
	SR-7 (b)	AU	AUDITABLE EVENTS	The COAS System Components must log, detect in a standard format and recorded in a time-stamped system-wide audit trail, the following events: a) actions performed by users and peer services accessing the applications; b) modification, or deletion of COAS data; c) information associated with logging in; d) information related to Communication Sessions and associated end points; e) events identifying connections (or attempts to connect) to the COAS Services;	AU-2

SR-8		AU	CONTENT OF AUDIT RECORDS	The COAS Audit Records must include: a) description of audit event occurred; b) when (date and time) the audit event occurred; e) previous and changed value of altered / deleted data; and f) the identity of the user associated with the audit event.	AU-3
SR-9		AU	AUDIT RECORD RETENTION	The Contractor must retain COAS Audit Records for a calendar year.	AU-11
SR-10	SR-10 (a)	CA	PLAN OF ACTION AND MILESTONES	The Contractor must develop a Plan of Actions and Milestones within 20 FGWDS of a request from Canada after the Service Readiness deliverable is accepted, that: a) documents the remedial actions planned by the Contractor to correct Vulnerabilities and security deficiencies identified during the Security Assessment and in any subsequent SOC2 Type II report or ISO re-certification; ; b) includes a Project Schedule to complete the remedial actions; and c) is approved by Canada.	CA-5
	SR-10 (b)			The Contractor must update the Plan of Actions and Milestones based on the results from security assessments, security impact analyses, and security monitoring activities conducted by the Contractor.	
	SR-10 (c)			The Contractor must implement the remedial actions identified in the Plan of Actions and Milestones in accordance with the Project Schedule for the initial approved version and any subsequent versions.	
SR-11		CM	CONFIGURATION MANAGEMENT	All hardware and software components of the Service must be registered in a Configuration Management Database (CMDB) as Configuration Items (CIs).	CM-2
SR-12	SR-12 (a)	CM	SECURITY IMPACT ANALYSIS	The Contractor must ensure all changes to the Service are tested in a pre-production environment prior to deployment into the production environment.	CM-4
	SR-12 (b)			The Contractor must test the Security Functions after a change in a pre-production environment to verify that the Security Functions are implemented correctly, operating as intended, and producing the desired outcome.	
SR-13		CM	LEAST FUNCTIONALITY	The Contractor must ensure that the COAS System Components are installed and maintained in a security-hardened configuration.	CM-7
SR-14		CP	CONTINGENCY PLAN	The Contractor must provide a 7/24/365 Service Desk if the Service Portal is unavailable for the following: a) Open Incidents; b) Create, change or cancel Audio / Web Conferences; and c) Create, change or cancel Service Requests.	CP-2
SR-15		CP	INFORMATION SYSTEM BACKUP	The Contractor must implement backups of Service Portal Data and COAS System Components to support recovery from Service failures.	CP-9
SR-16		CP	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The Contractor must provide the recovery and reconstitution of the Service from backup to an operational known state after a disruption, compromise, or failure in as per SLT-MTTR-COAS and SLT-MTTR-SP.	CP-10
SR-17		IA	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	The Service Participants must be uniquely identified when accessing COAS Services.	IA-2

SR-18		IA	IDENTIFIER MANAGEMENT	The Contractor must: a) identify Account Holders by their unique e-mail address; and b) e-mail addresses must be unique per Account Holder;	IA-4
SR-19	SR-19 (a)		AUTHENTICATOR MANAGEMENT	COAS Services Participants must be authenticated by email address provided in the reservation.	IA-5
	SR-19 (b)			The Contractor must authenticate e-mail addresses for Account Holders (e.g. confirmation e-mail).	
	SR-19 (c)			The Contractor must enforce the following password processes for COAS System Component Accounts: a) initial temporary passwords are changed upon the first logon; b) password meets all of the following criteria: i) contain at least 8 characters; ii) cannot reuse the same password for 4 iterations; iii) contains at least three of the following four character groups: A) English uppercase characters (A through Z); B) English lowercase characters (a through z); C) numerals (0 through 9); D) non-alphabetic characters (e.g., !, $, #, %);	
	SR-19 (d)			The Contractor must enforce the following password processes for Service Portal Accounts for Service Portal users: a) must ensure that initial temporary passwords are changed upon the first logon; b) must ensure that users creating a password meet the minimum complexity requirements and all of the following criteria: i) must contain at least 8 characters; ii) cannot reuse the same password for 4 iterations; iii) must contain at least three of the following four character groups: A) English uppercase characters (A through Z); B) English lowercase characters (a through z); C) numerals (0 through 9); D) non-alphabetic characters (e.g.,: !, $, #, %);	
	SR-19 (e)			The Contractor must encrypt all passwords for COAS in both transit and at rest. The Contractor must prevent offline attack measures (i.e. hashing, salting, keyed-hashing) for stroed passwords. Encryption algorithms must be recommnded by the Advanced Encryption Standard (AES) algorithm (as specified in National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 197: Advanced Encryption Standard) with key lengths of a minimum of 128 bits.	
SR-20	SR-20 (a)	IR	INCIDENT HANDLING	The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious emails) to protect COAS Services against cyber threats.	IR-4

	SR-20 (b)			The Contractor must perform the following activities when handling a Security Incident: a) analysis of scope, impact, source, and nature; b) choosing a containment and evidence gathering strategy, and executing the strategy; c) elimination of affected COAS System Components and mitigating any known Security Vulnerabilities; d) preparation of work flows, processes and training necessary to handle and prevent re-occurrence; e) restoration of COAS System Components to normal operations and remediating where necessary; f) preparation and delivery of information to applicable recipients (i.e. PSEPC, Law Enforcement, etc.); and g) identification and understanding of the root cause; and h) recording and preserving associated artifacts associated (e.g. lesson learned, approach, characteristics, etc.)	
SR-21	SR-21 (a)	IR	INCIDENT REPORTING	The Contractor must report all suspected or actual Security Incidents related to the Service to the TA within 5 FWCDs	IR-6
	SR-21 (b)			The Contractor must provide a Security Incident post-mortem report to Canada, within 72 hours of a request by Canada, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with Service; and j) recommendations to improve Service.	
SR-22	SR-22 (a)	IR	INCIDENT RESPONSE PLAN	The Contractor must implement an audit and investigation process for Security Incidents that allows only specific, pre-authorized representatives of Canada to request and receive discrete access and information associated with COAS Data for the purposes of conducting security investigations	IR-8
	SR-22 (b)			The Contractor must ensure the use of proper forensic procedures and safeguards for handling Security Incidents that includes the maintenance of a chain of custody for both the audit information.	
SR-23		MA	CONTROLLED MAINTENANCE	The Contractor must perform Release and Change Management for maintenance of the COAS System Components by: a) using Release and Change management processes for COAS Services and Service Portal in accordance with manufacturer or supplier specifications; b) testing all Changes in a pre-production environment prior to Production.	MA-2
SR-24		MP	MEDIA STORAGE	The Contractor must protect media storing COAS Data, including Portable Devices, until they are sanitized or destroyed.	MP-4
SR-25		PE	PHYSICAL ACCESS AUTHORIZATIONS	The Contractor must provide controlled physical access to the Service hosting facilities.	PE-2
SR-26		PE	PHYSICAL ACCESS CONTROL	The Contractor must implement controlled physical access to the Service hosting facilities.	PE-3
SR-27		PS	THIRD-PARTY PERSONNEL SECURITY	The Contractor must provide and implement physical access security controls for third party access to hosting facilities.	PS-7
SR-28		RA	RISK ASSESSMENT	The Contractor must implement all security patches through Change and Release Management Processes that are responsive to industry accepted Threat monitoring activities and result in timely mitigations to new and updated Threats.	RA-3

SR-29		RA	VULNERABILITY SCANNING	The Contractor must perform vulnerability assessment against COAS System Components for the purpose of discovering Security Vulnerabilities in the COAS Service and Service Portal: a) before hosting COAS Data; and b) on an annual basis.	RA-5
SR-30		SA	EXTERNAL INFORMATION SYSTEM SERVICES	The Contractor must ensure that subcontractors comply with the Security Control Requirements for the Service.	SA-9
SR-31		SC	BOUNDARY PROTECTION	The Contractor must implement a defense-in-depth approach for network protection (e.g. data confidentiality, data in transit protection, data integrity), logical and physical domain separation, network access control, and Boundary Protection appropriate for the data handled by the network following industry best practices related to network zoning and segmentation practices.	SC-7
SR-32		SC	NETWORK DISCONNECT	The Contractor must manage all network connections between COAS System Components and External Services as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); and c) terminate the network connection associated with a Communications Session at the end of the Communications Session or after minimum 10 minutes of inactivity;	SC-10
SR-33		SC	MOBILE CODE	The Contractor must authorize, and control the use of Mobile Code within the Service.	SC-18
SR-34		SC	SESSION AUTHENTICITY	The Service must establish and maintain the authenticity of Communication Sessions by recognizing only system-generated unique Session Identifiers and invalidating Session Identifiers upon Communication Session termination.	SC-23
SR-35		SI	FLAW REMEDIATION	The Contractor must implement a systematic patch management process to ensure that security-related patches, service packs, hot fixes, and Malware signatures are applied in a timely manner, this includes: a) ensuring the latest version of applications and operating systems are used; b) ensuring that vendor-supplied security patches are tested and applied in a timely manner; c) prioritizing critical patches and service packs against Common Vulnerabilities Scoring System (CVSS) v2 or similar Industry standard; and d) a testing and verification methodology to ensure that patches have been implemented properly.	SI-2
SR-36		SI	MALICIOUS CODE PROTECTION	The Contractor must implement, centrally manage, and periodically test, Malicious Code Protection mechanisms, that receive timely updates to virus definition files, on all COAS System Components in order to scan for the presence of Malware.	SI-3
SR-37		MP	MEDIA STORAGE	The Contractor must ensure that Canada's data (i.e. Protected A, or Classified) will only be processed and stored in a GC-approved computing facility located within the geographic boundaries of Canada or within the premises of a GC department located abroad, such as a diplomatic or consular mission.	CP-6, CP-9, MP-2, MP-7 & PE-3

Shared Services Canada

Conferencing & Operator Assisted Service (COAS)

Appendix 1 to Annex G

Supply Chain Security Information Assessment Process

Version 1.0

Table of Contents

1 Supply Chain Security Information Assessment Process

1.1 Condition of Contract Award:

Canada has determined that a thorough assessment of the supply chain associated with the goods and services to be acquired under this solicitation is critical to Canada's national security. To protect information associated with this process, unless Canada has invoked the National Security Exception with respect to this procurement, Canada relies on the exception provided in all trade agreements regarding its right not to disclose certain information where doing so would be contrary to the public interest. That information is identified below. In order to be awarded a contract, the Bidder must complete the Supply Chain Security Information (SCSI) assessment process and not be disqualified.

1.2 Definitions

The following words and expressions used with respect to SCSI assessment have the following meanings:

"Product" means any hardware that operates at the data link layer of the Open Systems Interconnection model (OSI Model) Layer 2 and above; any software; and any Workplace Technology Device;

"Workplace Technology Device" means any desktop, mobile workstation (such as a laptop or tablet), smart phone, or phone, as well as any peripheral item or accessory such as a monitor, keyboard, computer mouse, audio device or external or internal storage device such as a USB flash drive, memory card, external hard drive or writable CDs and DVDs or other media;

"Product Manufacturer" means the entity that assembles the component parts to manufacture the final Product;

"Software Publisher" means the owner of the copyright of the software, who has the right to license (and authorize others to license/sub-license) its software products;

"Canada's Data" means any data originating from the Work, any data received in contribution to the Work or any data that is generated as a result of the delivery of security, configuration, operations, administration and management services, together with any data that would be transported or stored by the contractor or any subcontractor as a result of performing the Work under any resulting contract; and

"Work" means all the activities, services, goods, equipment, matters and things required to be done, delivered or performed by the contractor under any resulting contract.

1.3 Bid Submission Requirements (Mandatory at Bid Closing):

Bidders must submit with their bids, by the closing date, the following:

a) **Ownership Information** for the Bidder and each of the Original Equipment Manufacturers (OEMs) selected by the Bidder and subcontractors including:

   i. Provide their Dunn & Bradstreet number, or:

   ii. Investors/Shareholders Information:

b) For privately owned companies, the Bidder must provide a list of all its shareholders. If the company is a subsidiary, this information must be provided for all parent corporations.

c) For publicly traded companies, the Bidder must provide a list of those shareholders who hold at least 1% of the voting shares;

d) Further information about other shareholders must be provided if requested by Canada;

e) A list of all executive level managers (e.g., chief executive officer (CEO), chief financial officer (CFO), chief operating officer (COO), and chief information officer (CIO) (and further information about the members of the Board of Directors must be provided if requested by Canada); Board of Directors (and further information about the members of the Board of Directors must be provided if requested by Canada);

f) In the case of partnerships, a list of all the partners (and further information about the partners must be provided if requested by Canada); and

g) In the case of a joint venture, the above information must be provided for each member of the joint venture; and

h) Corporate Website link.

1.4 IT Product List

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

a) **OEM**: identify the name of the Original Equipment Manufacturer (OEM).

b) **Product Code**: Enter the OEM's code for the product.

c) **Product Family or Product Model Name/Number**: identify the advertised family or name/number of the Product assigned to it by the OEM;

d) **Product Website Link**: A URL to the product family on the OEM's website, or a URL to the OEM's specific model and version.

e) **Vulnerability Information**: If the OEM participates in the Common Vulnerability Enumeration (CVE) disclosure process, provide the 5 most recent CVE identifiers in a semi-colon (;) separated list. If the OEM has alternative methods to report security vulnerabilities to customers, the 5 more recent advisories / bulletins from the vendor, related to the Model / Version in question, must be provided. Submitting the information set out above is mandatory. Canada requests that Bidders provide the IT Product List information by using the SCSI Submission Form, but the form in which the information is submitted is not itself mandatory. Canada also requests that, on each page, Bidders indicate their legal name and insert a page number as well as the total number of pages. Canada further requests that Bidders insert a separate row in the SCSI Submission Form for each Product. Finally, Canada requests that Bidders not repeat multiple iterations of the same Product (e.g., if the serial number and/or the color is the only difference between two Products, they will be treated as the same Product for the purposes of SCSI).

1.5 Assessment of Supply Chain Security Information

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

In conducting its assessment:

a) Canada may request from the Bidder any additional information that Canada requires to conduct a complete security assessment of the SCSI. The Bidder will have 2 working days (or a longer period

if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being disqualified.

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

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

a) Canada will notify the Bidder in writing (sent by email) and identify which aspect(s) of the SCSI is subject to concern(s) or cannot be assessed (for example, proposed future releases of products cannot be assessed). Any further information that Canada might be able to provide to the Bidder regarding its concerns will be determined based on the nature of the concerns. In some situations, it will not be in the public interest for Canada to provide further information to the bidder; therefore, in some circumstances, the bidder will not know the underlying reasons for Canada's concerns with respect to a product, subcontractor or other aspect of the bidder's SCSI (either during this process of following the award of any contract).

b) The notice will provide the Bidder with a minimum of 3 opportunities to submit revised SCSI in order to address Canada's concerns. The first revised SCSI must be submitted within the **10 calendar days** following the day on which Canada's written notification is sent to the Bidder (or a longer period specified in writing by the Contracting Authority). If concerns are identified by Canada regarding the first revised SCSI submitted after bid closing, the second revised SCSI must be submitted within **5 calendar days** (or a longer period specified in writing by the Contracting Authority). If concerns are identified by Canada regarding the second revised SCSI submitted after bid closing, the third revised SCSI must be submitted within **3 calendar days** (or a longer period specified in writing by the Contracting Authority). **With respect to the revised SCSI submitted each time, the Bidder must indicate in its response whether the revision affects any aspect of its technical bid or certifications. The Bidder will not be permitted to change any price in its bid but will be permitted to withdraw its bid if it does not wish to honour the pricing as a result of required revisions to the SCSI.** Each time the Bidder submits revised SCSI within the allotted time, Canada will perform a further assessment of the revised SCSI and the following will apply:

i. If, in Canada's opinion, there is a possibility that any aspect of the Bidder's revised SCSI could compromise or be used to compromise the security of Canada's equipment, firmware, software, systems or information, the Bidder will be provided with the same type of notice described under paragraph (e)(iii)(A) above. If, in Canada's opinion, the third post-bid-closing revised SCSI submission still raises concerns, any further opportunities to revise the SCSI will be entirely at the discretion of Canada and the bid may be disqualified by Canada at any time.

ii. If the bid is not disqualified as a result of the assessment of the SCSI (as revised in accordance with the process set out above), after receiving the final revised SCSI, Canada will assess the impact of the collective revisions on the technical bid and certifications to determine whether they affect:

iii. the Bidder's compliance with the mandatory requirements of the solicitation;

iv. the Bidder's score under the rated requirements of the solicitation, if any; or

v. the Bidder's ranking vis-à-vis other Bidders in accordance with the evaluation process

described in the solicitation.

vi. If Canada determines that the Bidder remains compliant and that its ranking vis-à-vis other Bidders has been unaffected by the revisions to the SCSI submitted after bid closing in accordance with the process described above, the Contracting Authority will recommend the top-ranked bid for contract award, subject to the provisions of the bid solicitation.

vii. If Canada determines that, as a result of the revisions to the SCSI submitted after bid closing in accordance with the process described above, the Bidder is either no longer compliant or is no longer the top-ranked Bidder, Canada will proceed to consider the next-ranked bid for contract award, subject again to the provisions of the solicitation relating to the assessment of the SCSI submitted at bid closing, and to the assessment of any revised SCSI submitted after bid closing in accordance with the above provisions.

c) By participating in this process, the Bidder acknowledges that the nature of information technology is such that new vulnerabilities, including security vulnerabilities, are constantly being identified. As a result:

i. a satisfactory assessment does not mean that the same or similar SCSI will be assessed in the same way for future requirements; and

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

d) By submitting its SCSI, and in consideration of the opportunity to participate in this procurement process, the Bidder agrees to the terms of the following non-disclosure agreement (the "Non-Disclosure Agreement"):

i. The Bidder agrees to keep confidential and store in a secure location any information it receives from Canada regarding Canada's assessment of the Bidder's SCSI (the "Sensitive Information") including, but not limited to, which aspect of the SCSI is subject to concern, and the reasons for Canada's concerns.

ii. Sensitive Information includes, but is not limited to, any documents, instructions, guidelines, data, material, advice or any other information whether received orally, in printed form or otherwise, and regardless of whether or not that information is labeled as classified, confidential, proprietary or sensitive.

iii. The Bidder agrees that it will not reproduce, copy, divulge, release or disclose, in whole or in part, in whatever way or form any Sensitive Information to any person other than a person employed by the Bidder who has a need to know the information and has a security clearance commensurate with the level of Sensitive Information being disclosed, without first receiving the written consent of the Contracting Authority.

iv. The Bidder agrees to notify the Contracting Authority immediately if any person, other than those permitted by the previous Sub-article, accesses the Sensitive Information at any time.

v. The Bidder agrees that a breach of this Non-Disclosure Agreement may result in disqualification of the Bidder at any stage of the procurement process, or immediate termination of a resulting contract or other resulting instrument. The Bidder also acknowledges that a breach of this Non-Disclosure Agreement may result in a review of the Bidder's security clearance and a review of the Bidder's status as an eligible Bidder for other requirements.

vi. All Sensitive Information will remain the property of Canada and must be returned to the

Contracting Authority or destroyed, at the option of the Contracting Authority, if requested by the Contracting Authority, within 30 days following that request.

vii. This Non-Disclosure Agreement remains in force indefinitely. If the Bidder wishes to be discharged from its obligations with respect to any records that include the Sensitive Information, the Bidder may return all the records to an appropriate representative of Canada together with a reference to this Non-Disclosure Agreement. In that case, all Sensitive Information known to the Bidder and its personnel (i.e., Sensitive Information that is known, but not committed to writing) would remain subject to this Non-Disclosure Agreement, but there would be no further obligations with respect to the secure storage of the records containing that Sensitive Information (unless the Bidder created new records containing the Sensitive Information). Canada may require that the Bidder provide written confirmation that all hard and soft copies of records that include Sensitive Information have been returned to Canada.

The Bidders must complete the COAS Mandatory Technical Requirements Evaluation Forms, which comprises of:
a. evidence of experiences, and;
b. evidence of their understanding of the requirements contained in the Annexes A, B, and C.

Bidders must provide past experience for Mandatories M-1, M-2, M-3, and M-4, as well as Customer Reference projects and customer contacts for the services delivered.

The Customer References, for each Service Project, must clearly attest to having used the Service Portal in both of Canada's Official Languages (English and French). For greater clarity, if the Customer Reference can only attest to using the Service Portal in one of Canada's Official Languages, the Bidder must provide another Customer Reference who can attest to using the Service Portal in the remaining Official Language of Canada.

For mandatory R-1, Bidders are required to demonstrate their ability to execute the requirements contained in the Annexes A, B and C by providing Design Documentation including an Implementation Plan for R1-01, R1-02, and R1-03.

Canada requires that bidders present a design that meets the requirements of Annex A, B and C in response to R1. Bidders should demonstrate in their Design Documentation their technical capabilities, their technical expertise, and their technical understanding of the design requirements in a detailed, thorough, concise and clear manner. The technical bid should provide design details (i.e. architecture, diagrams, models, descriptions, etc.) of their technical solution which are subject to the mandatory evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient.

The three top ranked Bidders will be required to provide a demonstration to Canada of the COAS Services as outlined in the "Demo" tab of this workbook to verify compliance. The demo is a pass/fail rating. If the Bidder fails the demonstration - Canada will proceed to the second ranked Bidder, at Canada's sole discretion.

Mandatory Experience Requirement M-1 **Service Portal**		**Evaluation**	**Comments**
The Bidder must have built and have experience providing a Service Portal to deliver two separate "Service Projects" to at least one customer over a minimum of 12 continuous months (per Service Project) in the 5 years prior to the bid closing date that meets all of the following criteria: (a) provided to the customer in both of Canada's Official Languages (English and French); (b) accessible online, 24 hours per day, 7 days per week, 365 days per year (24x7x365) from the Internet using a web browser; (c) requires secure login by (minimum) username and password authentication; and (d) includes, at a minimum the following functionalities: - RBAC for defined roles, views, permissions for Service Portal access; - Creating, modifying and cancelling orders for Services; - incident reporting; - service operations reporting; - status reporting; - billing and invoicing; and - documentation management. For greater clarity, it is not acceptable to Canada that one Service Project is provided to a customer in English only and another Service Project is provided to a customer in French only. Each Service Project must be provided to the customer in both English and French. To respond to M-1, the Bidder must complete all sections under both "Service Project #1" and "Service Project #2" below. In so doing, the Bidder must clearly, and in sufficient detail, describe how the experience meets all of the criteria listed above in M-1. To substantiate the Bidder's experience described in each Service Project, the Bidder must submit adequate documentation (e.g. user manual) of the Service Portal to demonstrate the above criteria. The Customer References, for each Service Project, **must clearly attest to** having used the Service Portal in both of Canada's Official Languages (English and French). For greater clarity, if the Customer Reference can only attest to using the Service Portal in one of Canada's Official Languages, the Bidder must provide another Customer Reference who can attest to using the Service Portal in the remaining Official Language of Canada.		For evalutation purposes only.	
Service Project #1			
Name of Service			
Description of Service			
M-1 (a) provided to the customer in both of Canada's Official Languages (English and French);			
M-1 (b) accessible online, 24 hours per day, 7 days per week, 365 days per year (24x7x365) from the Internet using a web browser;			
M-1 (c) requires secure login by (minimum) username and password authentication			
M-1 (d) includes, at a minimum the following functionalities: - RBAC for defined roles, views, permissions for Service Portal access; - Creating, modifying and cancelling orders for Services; - incident reporting; - service operations reporting; - status reporting; - billing and invoicing; and - documentation management.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Service Project #2			
Name of Service			
Description of Service			
M-1 (a) provided to the customer in both of Canada's Official Languages (English and French);			
M-1 (b) accessible online, 24 hours per day, 7 days per week, 365 days per year (24x7x365) from the Internet using a web browser;			
M-1 (c) requires secure login by (minimum) username and password authentication			

M-1 (d) includes, at a minimum the following functionalities: - RBAC for defined roles, views, permissions for Service Portal access; - Creating, modifying and cancelling orders for Services; - incident reporting; - service operations reporting; - status reporting; - billing and invoicing; and - documentation management.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
	Summary		
	Additional Customer Reference for Service Project 1 or/and 2 (If Required)		
Name of Service			
Description of Service			
M-1 (a) provided to the customer in both of Canada's Official Languages (English and French);			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer) - If required for additional language	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)- If required for additional language	**Name**		
	Telephone Number		
	Email Address		

Mandatory Experience Requirement M-2 **Operator Assisted Service (OAS)**		**Evaluation**	**Comments**
The Bidder, or at least one member of its joint venture or the bidders committed subcontractor must have experience providing at least two different projects for an Operator Assisted Service (each an "OAS Project") to at least two customers over a minimum of 6 continuous months (per OAS Project) in the 3 years prior to the bid closing date that meets all of the following criteria: (a) is provided to the customer in both of Canada's Official Languages (English and French); (b) uses an audio or web application or both; (c) Mobile enabled; (d) PTSN enabled; (e) Integrated VoIP connectivity enabled; (f) Provides all of the following 24 hours per day, 7 days per week, 365 days per year (24x7x365) as per the description of each of the following in Table 1 of Annex C, Section 1 - Press briefings ; - Q&A sessions; and - Virtual events. To respond to M-2, the Bidder or its committed subcontractor must complete all sections under both "OAS Project #1" and "OAS Project #2" below. In so doing, the Bidder must clearly, and in sufficient detail, describe how the experience meets all of the criteria listed above in M-2. Please provide the following information for two (2) OAS Projects that you have delivered to two separate customers to demonstrate this requirement. The Customer References, for each OAS Project, must clearly attest to having use the OAS in both of Canada's Official Languages (English and French).		For evalutation purposes only.	
OAS Project #1			
Name of Service			
Legal Name of Provider (either the Bidder or its subcontractor)			
Description of Service			
M-2 (a) is provided to the customer in both of Canada's Official Languages (English and French;			
M-2 (b) uses an audio or web application or both;			
M-2 (c) Mobile enabled;			
M-2 (d) PTSN enabled			
M-2 (e) Integrated VoIP connectivity enabled			
M-2 (f) Provides all of the following 24 hours per day, 7 days per week, 365 days per year (24x7x365]: - Press briefings; - Q&A sessions; and - Virtual events.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
OAS Project #2			
Name of Service			
Legal Name of Provider (either the Bidder or its subcontractor)			
Description of Service			
M-2 (a) is provided to the customer in both of Canada's Official Languages (English and French;			
M-2 (b)auses an audio or web application or both;			
M-2 (c) Mobile enabled;			
M-2 (d) PTSN enabled			
M-2 (e) Integrated VoIP connectivity enabled			

M-2 (f) Provides all of the following 24 hours per day, 7 days per week, 365 days per year (24x7x365): - Press briefings; - Q&A sessions; and - Virtual events.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		

	Additional Customer Reference for Service Project 1 or/and 2 (If Required)
Name of Service	
Description of Service	
M-1 (a) provided to the customer in both of Canada's Official Languages (English and French);	
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)	
Start Date of Service Project ***[Enter dd/mm]***	
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***	
Customer Reference #1 (Primary Contact for the Customer) - If required for additional language	**Name**
	Telephone Number
	Email Address
Customer Reference #2 (Backup Contact for the Customer)- If required for additional language	**Name**
	Telephone Number
	Email Address

Mandatory Experience Requirement M-3 **Audio and Web Conferencing Services** (For M-3, the Bidder may rely on the experience of third parties whom the Bidder proposes to use at its subcontractors for COAS.) The Bidder or its committed subcontractor or both must have experience providing at least two different projects for an Audio and Web Conferencing Service (each an "AWS Project") to at least two customers over a minimum of 6 continuous months (per AWS Project) in the 3 years prior to bid closing that meets all of the following criteria: (a) is provided to the customer in both of Canada's Official Languages (English and French); and (b) accessible online, 24 hours per day, 7 days per week, 365 days per year (24x7x365) from the Internet using a web browser or web application to: i. schedule, modify, or cancel meetings ii. have a capacity of a minimum of 3000 participants; iii. provide a Webcasting functionality; iv. provide Closed Captioning in both of Canada's Official Languages; and v. allow integration of PSTN and VoIP calls. To respond to M-3, the Bidder must complete all sections under both "AWS Project #1" and "AWS Project #2" below. In so doing, the Bidder or its committed subcontractor must clearly, and in sufficient detail, describe how the experience meets all of the criteria listed above in M-3. Please provide the following information for two (2) AWS Projects that you have delivered to customers to demonstrate this requirement. The Customer References, for each AWS Project, must clearly attest to having used the AWS in both of Canada's Official Languages (English and French).		**Evaluation** For evalutation purposes only.	**Comments**
AWS Project #1			
Name of Service			
Legal Name of Provider (either the Bidder or its subcontractor)			
Description of Service			
M-3 (a) is provided to the customer in both of Canada's Official Languages (English and French; M-3 (b) accessible online, 24 hours per day, 7 days per week, 365 days per year (24x7x365) from the Internet using a web browser or web application to: i. schedule, modify, or cancel meetings ii. have a capacity of a minimum of 3000 participants; iii. provide a Webcasting functionality; iv. stream content to social media; v. provide Closed Captioning in both of Canada's Official Languages; and vi. allow integration of PSTN and VoIP calls.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project *[Enter dd/mm]*			
End Date of Service Project *[Enter dd/mm/yyyy or "ongoing"]*			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
AWS Project #2			
Name of Service			
Legal Name of Provider (either the Bidder or its subcontractor)			
Description of Service			
M-3 (a) is provided to the customer in both of Canada's Official Languages (English and French; M-3 (b) accessible online, 24 hours per day, 7 days per week, 365 days per year (24x7x365) from the Internet using a web browser or web application to: i. schedule, modify, or cancel meetings ii. have a capacity of a minimum of 3000 participants; iii. provide a Webcasting functionality; iv. stream content to social media; v. provide Closed Captioning in both of Canada's Official Languages; and vi. allow integration of PSTN and VoIP calls.			

Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		

Additional Customer Reference for Service Project 1 or/and 2 (If Required)	
Name of Service	
Description of Service	
M-1 (a) provided to the customer in both of Canada's Official Languages (English and French);	
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)	
Start Date of Service Project ***[Enter dd/mm]***	
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***	
Customer Reference #1 (Primary Contact for the Customer) - If required for additional language	**Name**
	Telephone Number
	Email Address
Customer Reference #2 (Backup Contact for the Customer)- If required for additional language	**Name**
	Telephone Number
	Email Address

Mandatory Experience Requirement M-4 **Service Desk**		**Evaluation**	**Comments**
The Bidder must demonstrate experience in providing at least two separate projects involving a Service Desk (each a "Service Desk Project") to at least two different customers for at least 6 continuous months during the 2 years prior to bid closing that meets all of the following criteria providing: (a) customer in both of Canada's Official Languages (English and French); and (b) available 24 hours per day, 7 days per week, 365 days per year (24x7x365) (c) accessible by: i. local phone number; ii. toll-free number; iii. PSTN call * touch feature; and iv. live chat; (d) conferencing technical support; (e) scheduling and service request support; and (f) incident management support. To respond to M-4, the Bidder must complete all sections under both "Service Desk Project #1" and "Service Desk Project #2" below. In so doing, the Bidder or its committed subcontractor must clearly, and in sufficient detail, describe how the experience meets all of the criteria listed above in M-4.		For evalutation purposes only.	
Service Desk Project #1			
Name of Service			
Legal Name of Provider (either the Bidder or its subcontractor)			
Description of Service			
M-4 (a) is provided to the customer in both of Canada's Official Languages (English and French);			
M-4 (b)available 24 hours per day, 7 days per week, 365 days per year (24x7x365)			
M-4 (c)accessible by: i. local phone number; ii. toll-free number; iii. PSTN call * touch feature; and iv. live chat;			
M-4 (d) conferencing technical support			
M-4 (e) scheduling and service request support; and			
M-4 (f) incident management support.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Service Desk Project #2			
Name of Service			
Legal Name of Provider (either the Bidder or its subcontractor)			
Description of Service			
M-4 (a) is provided to the customer in both of Canada's Official Languages (English and French);			
M-4 (b)available 24 hours per day, 7 days per week, 365 days per year (24x7x365)			

M-4 (c) accessible by: i. local phone number; ii. toll-free number; iii. PSTN call * touch feature; and iv. live chat;			
M-4 (d) conferencing technical support			
M-4 (e) scheduling and service request support; and			
M-4 (f) incident management support.			
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)			
Start Date of Service Project ***[Enter dd/mm]***			
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***			
Customer Reference #1 (Primary Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		
Customer Reference #2 (Backup Contact for the Customer)	**Name**		
	Telephone Number		
	Email Address		

	Additional Customer Reference for Service Project 1 or/and 2 (If Required)
Name of Service	
Description of Service	
M-1 (a) provided to the customer in both of Canada's Official Languages (English and French);	
Name of Customer organization for whom work was performed (the entity claiming the experience must have had a contract directly with the customer organization)	
Start Date of Service Project ***[Enter dd/mm]***	
End Date of Service Project ***[Enter dd/mm/yyyy or "ongoing"]***	
Customer Reference #1 (Primary Contact for the Customer) - If required for additional language	**Name**
	Telephone Number
	Email Address
Customer Reference #2 (Backup Contact for the Customer)- If required for additional language	**Name**
	Telephone Number
	Email Address

Rated Requirement R-1

Design Documentation Requirement for COAS Implementation

(1) The technical bid must include the Design Documentation listed in R-1 that evidence the Bidder's understanding of the COAS Statements of Work, Annexes A (COAS-General Statement of Work), Annex B (AWS) and Annex C (OAS).

(2) In preparing its Design Documentation, the Bidder should not make any assumptions regarding Work to be performed by Canada unless the Annexes A, B and C (inclusive of all appendices) already indicates that certain functions will be performed by Canada. The Bidders should ask questions if they are not certain whether certain functions will be performed by Canada or not. If a Bidder's Design Documentation indicate that Canada will perform functions not specified in the Annexes A, B, and C (including all appendices), Canada will rate the Bidder accordingly, given that understanding the allocation of responsibilities is an important aspect of understanding the requirements.

(3) The Bidder must not make any assumptions (i.e. for timeline or design requirements) in the Design Documentation.

(4) Each Design Documentation Requirement will be assessed a Technical Criteria Score based on the extent to which the Design Documentation demonstrates the Bidder's understanding of the Statements of Work, Annexes A, B, and C, through an evaluation of its comprehensiveness and completeness as further described in the Technical Evaluation Worksheet.

(5) Canada will assess each Technical Criterion for Design Documentation Requirement based on 4 independent Technical Criteria Scores. The Technical Criteria Scores for each of the 3 specific Design Documentation requirements will be added to provide a single Technical Criteria Score for a maximum of 60 points of the Technical Mandatory Evaluation Requirements.

(6) The Draft RFP Posting Period must be used for any clarifications, if required. Questions or requests for one-on-one meetings can be submitted to the Contracting Authority exclusively during the Draft RFP Posting Period.

(7) The Technical Criteria relevant to each Design Documentation requirement are defined in the Technical Evaluation Worksheet.

Technical Criteria Scoring for Design Documentation Requirements

Level Of Understanding and Completeness	Description	Technical Criteria Score
EXCEPTIONAL Comprehensive Understanding and Completeness	The Bidder's Design Documentation has fully addressed the Technical Criteria and provided a high level of detail in accordance with the requirements described in the Statements of Work, Annexes A, B and C. The Design Documentation demonstrates a high degree of understanding of the Technical Criteria in accordance with the requirements described in Annexes A, B and C and is consistent with the remainder of the bid.	100% of maximum points available
ACCEPTABLE Adequate Understanding and Completeness	The Bidder's Design Documentation has generally addressed the Technical Criteria and provided an adequate level of detail in accordance with the requirements described in the Statements of Work, Annexes A, B and C. The Design Documentation demonstrates an adequate understanding of the Technical Criteria in accordance with the requirements described in the Annexes A, B and C and is consistent with the remainder of the bid.	75% of available points

MARGINAL Insufficient Understanding and Completeness	The Bidder's Design Documentation: a) does not sufficiently demonstrate an adequate degree of understanding of the Technical Criteria in accordance with the requirements described in the Statements of Work, Annexes A, B and C (the degree of understanding is deficient and could compromise the achievement of the contract requirements); b) does not provide an adequate level of detail in accordance with the requirements described in the Statements of Work, Annexes A, B and C (the level of detail is deficient and could compromise the achievement of the contract requirements); c) is not specific or tailored to the requirements described in the level of detail in accordance with the requirements described in the Statements of Work, Annexes A, B and C; or d) is not consistent with other sections of the bid.	50 % of available points
UNSATISFACTORY Lack of understanding or completion	The Bidder's Requirements Knowledge Document is either: a) missing; b) Incomplete in quality and quantity c) Evidences lack of understanding	0% of available points

Technical Criteria for Requirements Knowledge Documents

Technical Criteria ID	Requirements Knowledge Document / Technical Criteria	Available points	Supporting Documentation
R1-01	The Bidder must provide the COAS Implementation Plan. The Bidder must provide a draft of the COAS Implementation Plan as described in Annex A, Section 5.2 Implementation Plan and Milestones.	10	
R1-02	The Bidder must provide the COAS Service Portal Design Overview of SRS The Bidder must provide the COAS Service Portal Design Overview Document that demonstrates the Bidder's understanding and ability to deliver the Service Portal and SRS requirements as described in Annex A.	15	
R1-03	The Bidder must provide the COAS Service Design Overview of COAS Services The Bidder must provide the COAS Service Design Overview that demonstrates the Bidder's understanding and ability to deliver all COAS Services, features and functions as per Annex B and C, and must include the identification of any and all: a) OEM software; b) Subcontractors; c) Cloud Services; and d) Cloud Service Providers.	15	

Features	Description	YES	NO	Explanation
Scheduling	Host able to schedule meetings and send out meeting invitations through Microsoft Outlook.			
Registration	Ability for Participants to sign up for a conference in advance of the start date & time; providing the personal information requested by the conference Host or Co-Host and the ability for the Host or Co-Host to obtain information on who & how many Participants have signed up to attend the future conference.			
Audio only conference without operator assistance	A self serve audio conference initiated by the host.			
Audio only conference with operator assistance	An audio conference provided through the assistance of an operator.			
Webcasting functionality	A webcast is a media presentation distributed over the Internet using streaming media technology to distribute a single content source to many listeners/viewers simultaneously.			
Web Conference with operator assistance	A hybrid conference using the web conferencing platform and providing operator assistance.			
Bridge Call Back functionality	Allows a meeting Participant to initiate a call from within the Web Conferencing Meeting application platform to connect audio for the Participant's connection.			
Call out functionality	Allows a Participant to initiate a call, and subsequently connect an additional Participant to the audio conference.			
Call in functionality	Ability for Participants to connect to the conference by dialling a telephone number.			
Audio Integration	Provide a flexible integrated audio that allows conference Participants to independently choose their audio preference, Public Switched Telephone (PSTN) or Voice over Internet Protocol (VoIP), and enables the same simultaneous experience for all Participants regardless of connectivity preference.			
Selection of language of operation	Both participants and the host are able to select their preferred official language; English or Canadian French			
Closed Captioning (English and French)	Closed captioning and subtitling are both processes of displaying text on a television, video screen, or other visual display to provide additional or interpretive information.			
Real time translation (RTT)	Displays the Closed Captions in the alternate official language of Canada from the language being spoken. (ie. English -> French and French -> English).			
American Sign Language (ASL)	ASL is a complete and organized visual language that is expressed by both manual and nonmanual features.			
Simultaneous Interpretation (SI)	SI is when an interpreter translates the message from the source language to the target language in real-time.			
Recording	Digital record of a Web Conference content and Participant interactions. Storage of the recording directly on the Host's PC, or on a secure server that is part of the service, at the option of the Host and that a unique, password-protected URL is provided for access to the recording			
Share presentations	The ability for Host and Participants to share materials, whether uploaded or open on the individual's device, for others in the conference to view, including files with an audio component to be shared within the conference.			
Notes	A space within the conference where Participant(s) can take notes, meeting minutes, action items, etc. Notes can be saved and shared after the conference.			
Chat functionality	send or a receive text messages to a selected Participant, or to all Participants simultaneously.			
Participant List (during the session)	Visible list of all Participants in the Web Conference and the associated Combined Conferencing Service Audio Teleconference (if any), available to all Participants			
Attention tracking/status	A feature currently available in a Web Conference that allows Hosts to identify that Participants are engaged with the meeting. It provides indicators if an attendee has minimized the meeting window or brought another window in front of the meeting window and can generate a post meeting report with a summary of attentiveness.			
Q&A	A feature that allows any conference Participant to post or reply to any question or comment made during the meeting. It can be directed at the entire conference or a specific individual.			
Polling functionality	Provides real-time ability to record the opinion or vote of Participants			
Transcription	A written record of all words spoken during a conference and can be downloaded and shared if needed.			
Streaming	Ability to continually transmit audio and video content from a server to viewers, via social media sites, (e.g., YouTube, Facebook).			
Video enabled	A multi-point transmission of voice and video communication that allows multiple Participants to communicate in real-time where each Participant transmits a Unicast Stream and receives a combined Unicast Stream of other Participant's voice and video.			
Keyboard & mouse sharing control	Allows a Participant to move the cursor and type on a file being shared. The Participant that is sharing the file can regain control at any time.			
File sharing	The ability for the Host to transfer files to Participants before, during, or after the conference.			
Post conference survey	Displays a survey for Participants to complete after the conference ends either via a pop-up window or by redirecting the Participant to a website. Submitted survey results are available for the Host in the Host account's reports			
Lobby	A virtual environment where Participants to the conference can wait to be admitted by the Host of the meeting.			
Co-Host	An individual can be permitted to assume the role and privileges of the meeting Host. It can be designated when scheduling the conference or during any live meeting.			

Breakout Sessions	The ability to separate Participants into smaller groups within the meeting environment where they can collaborate, share ideas and move in or out of any session and/or return to the original meeting.
Guest Speaker/Panelist roles	A feature in any Web Conference that provides a unique invitation and privileges during the Web Conference. A panelist will be able to be seen and heard, view feedback, become a polling coordinator, manage polls and download or present files.
Virtual Labs	A feature currently within the any session that allow Participants in various geographical locations with remote computers set up as a virtual lab to conduct tests or simulations.
In-conference testing and grading	A feature currently in any session that allows Hosts to test and grade attendees on topis or concepts that have been introduced in your session. Allows Hosts to set the time limit, number of attempts and decide how the grade of the test is given.
Whiteboard	An interactive whiteboard is a display that reacts to input from a Participants or from other digital devices. It allows interactive real time sessions that include: i) viewing any action taking place while content is being edited and annotated by Participants; ii) dragging the pointer across the page and perform freehand drawing; iii) highlighting specific areas; iv) erasing content, inserting and modifying shapes (i.e., lines, arrows, squares, circles, etc.); v) undoing, redoing, copying, cutting and pasting content; and vi) saving the content of a whiteboarding session.
Participant list (post conference)	A list of all connections to the conference, identifying each connection by the personal data obtained when the connection is established such as; Name, telephone number, email address.
Destination URL post conference	Redirects Participants to a specific website (URL) after the conference ends. This may be to complete a survey and to direct Participants to additional information or resource materials .
Encryption	Ability to enable / disable all shared content is encrypted when transmitted between user and server machines, such that the content is viewable only by using PCs that are authenticated to the Service and are running the Web Conference Service software.

DRAFT

Conferencing & Operator Assisted Services (COAS){SCAO}

Bidder Name: "Bidder's Name"

April 2009

Bidder Instructions	
Section	**Instructions**
Title Page	The Bidder should enter its name in cell C15 on the Title Page.
All WORKSHEETS	These worksheets represent the Bidder's firm unit pricing. Bidder provides input in Green cells only, all other cells of the worksheets are for information and evaluation purposes. Bidders are welcome to familiarize themselves with the formulas used for evaluation purposes.
WORKSHEET 1: OAS Pricing	The Bidder must provide positive prices (no negative numbers) in all yellow cells. The Bidder acknowledges that any values in yellow cells other than a non-negative currency values (i.e.: $1.23) will be considered to be a price of $0.00 (i.e. negative values, Blank values, NULL values, 0, N/A, non numeric values, special characters, etc.). Definition of yellow cells is provided in the Legend Tab. Bidder Compliance measures have been provided. When a financial input value meets the financial compliance control the Bidder Compliance Assessment cell adjacent to the input cell will indicate "COMPLIANT" and "NON-COMPLIANT when compliance controls are not followed. These controls are established to avoid "gaming" the financial evaluation. If compliance controls are prohibitive to Bidder's response a question can be sent to clarify any requirement for the financial evaluation during the Q&A period of the RFP.
WORKSHEET 2: AWS Pricing	
WORKSHEET 3: Service Portal Pricing	
WORKSHEET 4: Optional Services	Bidders are welcome to familiarize themselves with the formulas used for evaluation purposes.
WORKSHEET 5. Financial Evaluation	Pricing data proposed by the Bidder WORKSHEETS 1 - 3 are used to determine the Bidder's Total Evaluated Bid Price. The evaluation spreadsheets will auto-populate from data entered into spreadsheets 1-3 inclusive. Bidders are welcome to familiarize themselves with the formulas used for evaluation purposes. "RFP Ranking" must be unique per bidder (i.e. no ties). If there is a tie, then to determine the unique ranking, 1 point will be added for the lowest price SCID that has the highest "Points per SCID" until the ranking can be determined as unique across all bidders.

Legend and details of each pricing cell		
SCID	Description	Compliance Control
OASCYxx	OAS Price per Minute per active port for meetings starting during core FGWD days of 8am to 7pm. OAS Services are described in Annex C.	Pricing must be a greater than 0 and within 10% of previous year otherwise bid will receive no further consideration
OASNYxx	OAS Price per Minute per active port for meetings starting during non-core FGWD days of 8am to 7pm. OAS Services are described in Annex C.	Pricing must be a greater than 0 and within 10% of previous year otherwise bid will receive no further consideration
OASCRNE	This is a flat fee per conference that can be charged to Canada if a new conference with OAS is created less than 30 minutes from the start time.	Pricing must be a greater than $0.00 and less than $100.00 otherwise bid will receive no further consideration
OASEMCE	This is a flat fee per conference that can be charged to Canada if the starting time of the OAS conference was scheduled within 30 minutes.	Pricing must be a greater than $0.00 and less than $100.00 otherwise bid will receive no further consideration
OASEMEE	This is a flat fee per conference that can be charged to Canada if the starting time of the OAS conference was scheduled more than 30 minutes but less than 120 minutes.	Pricing must be a greater than $0.00 and less than $100.00 otherwise bid will receive no further consideration
OASUNPE	Actual reserved ports is established at meeting start time. Ports that were reserved but had no usage on them at the end of conference are considered an unused port. The Contractor cannot charge for 10% or less of unused ports. The Contractor can charge for more than 10% of the unused ports as a per port charge.	Pricing must be a greater than $0.00 and less than $20.00 otherwise bid will receive no further consideration
AWAPPE	The Audio Web Annual License cost per Active User. This cost must be an "Active User Model" described in the Terms and Conditions and the AWS are described in Annex B.	Pricing must be a greater than $0.00 and less than previous year otherwise bid will receive no further consideration
AWRTTE	The Audio Web Annual License cost per Active User for real time translation. This cost must be an "Active User Model" described in the Terms and Conditions. The real time translation feature displays translated Closed Captioning from English to French or French to English in real time from the language being spoken.	Pricing must be a greater than $0.00 and less than $100.00 otherwise bid will receive no further consideration
SPG1	Price for delivering all requirements and obtaining Service Portal Gate Design Gate 1 approval as described in Annex 1.	Pricing must be a greater than $0.00 otherwise bid will receive no further consideration
SPG2	Price for delivering all requirements and obtaining Service Portal Gate Design Gate 2 approval as described in Annex 1.	Pricing must be a greater than $0.00 otherwise bid will receive no further consideration
SPG3	Price for delivering all requirements and obtaining Service Portal Gate Design Gate 3 approval as described in Annex 1.	Pricing must be a greater than $0.00 otherwise bid will receive no further consideration
SPCRExxx	The price for a Service Portal Feature change as described in Annex 1.	Pricing must be a greater than $0.00 and less than $20,000.00 otherwise bid will receive no further consideration
SPSCExxx	The price for a Service Portal Standard Change as described in Annex 1.	Pricing must be a greater than $0.00 and less than $7,500.00 otherwise bid will receive no further consideration
OPTxxx	Reserved for future use of optional features and functions of the COAS services.	N/A

WORKSHEET 1: OAS Pricing

Operator Assisted Service	8am to 7pm M-F Eastern Time - FGWDs		Compliance	Available 7pm to 8am local time, 7 days per week + non-FGWDs		Compliance
	SCID	Price per Minute per active port - Core hours		SCID	Price per Minute per active port - Non-Core hours	
OAS Price Year 1	OASCY01	**$1.00**	COMPLIANT	OASNY01	**$1.00**	COMPLIANT
OAS Price Year 2	OASCY02	**$1.00**	COMPLIANT	OASNY02	**$1.00**	COMPLIANT
OAS Price Year 3	OASCY03	**$1.00**	COMPLIANT	OASNY03	**$1.00**	COMPLIANT
OAS Price Year 4	OASCY04	**$1.00**	COMPLIANT	OASNY04	**$1.00**	COMPLIANT
OAS Price Year 5 - Option Year 1	OASCY05	**$1.00**	COMPLIANT	OASNY05	**$1.00**	COMPLIANT
OAS Price Year 6 - Option Year 2	OASCY06	**$1.00**	COMPLIANT	OASNY06	**$1.00**	COMPLIANT
OAS Price Year 7 - Option Year 3	OASCY07	**$1.00**	COMPLIANT	OASNY07	**$1.00**	COMPLIANT
OAS Price Year 8 - Option Year 4	OASCY08	**$1.00**	COMPLIANT	OASNY08	**$1.00**	COMPLIANT
OAS Price Year 9 - Option Year 5	OASCY09	**$1.00**	COMPLIANT	OASNY09	**$1.00**	COMPLIANT
OAS Price Year 10 - Option Year 6	OASCY10	**$1.00**	COMPLIANT	OASNY10	**$1.00**	COMPLIANT

Billable OAS Fees per Conference	SCID	Price	Compliance
Cancellation or Reschedule Fees < 24 hours (Flat fee per conference)	OASCRNE	$1.00	COMPLIANT
Emergency Conference Type 1 (scheduled < 30 minutes before start)	OASEMCE	$1.00	COMPLIANT
Emergency Conference Type 2 (scheduled >30 minutes but less than 120 minutes)	OASEMEE	$1.00	COMPLIANT

Billable OAS Fees per Unused Port	SCID	Price	Compliance
Unused port Fees >10% (Flat fee per port)	OASUNPE	$1.00	COMPLIANT

WORKSHEET 2: AWS Pricing

AUDIO WEB APPLICATION	SCID	Tier Pricing			
		Tier 1: 0-3,500 Active Users	Tier 2: 3501-6000 active Users	Tier 3: 6001 -7500 active Users	Tier 4: 7501+ active Users
Audio Web Annual License cost per Active User:	AWAPPE	**$1.00**	**$1.00**	**$1.00**	**$1.00**
Compliance		COMPLIANT	COMPLIANT	COMPLIANT	COMPLIANT

ADDITIONAL AUDIO WEB LICENSES	SCID	Price Per Active User
Real time translation (RTT) in both English and French	AWRTTE	**$1.00**
Compliance		COMPLIANT

WORKSHEET 3: Service Portal Pricing

Service Portal Gate	SCID	Service Portal Bid	Compliance
Service Portal Design Build Gate 1	SPG1	**$100,000.00**	COMPLIANT
Service Portal Design Build Gate 2	SPG2	**$125,000.00**	COMPLIANT
Service Portal Design Build Gate 3	SPG3	**$150,000.00**	COMPLIANT

Service Portal Changes	SCID	Ceiling Unit Price	Compliance
Feature Change (max price per full release cycle)	SPCRExxx	**$5,000.00**	COMPLIANT
Standard Change	SPSCExxx	**$1,000.00**	COMPLIANT

WORKSHEET 4: Optional Services

Optional (Services, Features, Functions) Name and complete Description	License Type and Restrictions	Reference (Appendix)	optinal / mandatory	SCID	Price Type	Price
				OPTE001		
				OPTE002		
				OPTE003		
				OPTE004		
				OPTE005		
				OPTE006		
				OPTE007		
				OPTE008		
				OPTE009		
				OPTE010		
				OPTE011		
				OPTE012		
				OPTE013		
				OPTE014		
				OPTE015		
				OPTE016		
				OPTE017		
				OPTE018		
				OPTE019		
				OPTE020		

WORKSHEET 5. Financial Evaluation

Score	Weight of RFP	"Bidder's Name"	<Bidder 2>	<Bidder 3>	<Bidder 4>	<Bidder 5>
OAS{SAO}	20	4.00	20.00	20.00	20.00	20.00
AWS	20	4.00	20.00	20.00	20.00	20.00
Service Portal	20	4.00	20.00	20.00	20.00	20.00
Total RFP Points	60	12.00	60.00	60.00	60.00	60.00
Financial Ranking		5	1	1	1	1

OAS Evaluation	OASCY01-10			OASNY01-10			OASCANE, OASRESE, OASEMCE, OASEMEE			OASUNPE		
Score Weight	45%			15%			15%			25%		
Points per respective SCID / Ranges	9			3			3			5		
Evaluation Metric	PRICE	RANK	SCORE	PRICE	RANK	SCORE	PRICE	RANK	SCORE	PRICE	RANK	SCORE
"Bidder's Name"	$10.00	5	1.80	$10.00	5	0.60	$3.00	5	0.60	$1.00	5	1.00
<Bidder 2>	$0.00	1	9.00	$0.00	1	3.00	$0.00	1	3.00	$0.00	1	5.00
<Bidder 3>	$0.00	1	9.00	$0.00	1	3.00	$0.00	1	3.00	$0.00	1	5.00
<Bidder 4>	$0.00	1	9.00	$0.00	1	3.00	$0.00	1	3.00	$0.00	1	5.00
<Bidder 5>	$0.00	1	9.00	$0.00	1	3.00	$0.00	1	3.00	$0.00	1	5.00

AWS Evaluation	AWAPPE			AWRTTE		
Score Weight	85%			15%		
Points per respective SCID / Ranges	17			3		
	PRICE	RANK	SCORE	PRICE	RANK	SCORE
"Bidder's Name"	$4.00	5	3.40	$1.00	5	0.60
<Bidder 2>	$0.00	1	17.00	$0.00	1	3.00
<Bidder 3>	$0.00	1	17.00	$0.00	1	3.00
<Bidder 4>	$0.00	1	17.00	$0.00	1	3.00
<Bidder 5>	$0.00	1	17.00	$0.00	1	3.00

Service Portal Evaluation	SPG1-3			SPCRExxx, SPSCExxx		
Score Weight	70%			30%		
Points per respective SCID / Ranges	14			6		
Bidder Name	PRICE	RANK	SCORE	PRICE	RANK	SCORE
"Bidder's Name"	$375,000.00	5	2.80	$1.00	5	1.20
<Bidder 2>	$0.00	1	14.00	$0.00	1	6.00
<Bidder 3>	$0.00	1	14.00	$0.00	1	6.00
<Bidder 4>	$0.00	1	14.00	$0.00	1	6.00
<Bidder 5>	$0.00	1	14.00	$0.00	1	6.00

DRAFT

Score		Weight of RFP	"Bidder's Name"	<Bidder 2>	<Bidder 3>	<Bidder 4>	<Bidder 5>
Financial Evaluation Ranking		60					
Technical Evaluation							
	M1		pass	pass	pass	pass	pass
	M2		pass	pass	pass	pass	pass
	M3		pass	pass	pass	pass	pass
	M4		pass	pass	pass	pass	pass
	R1-01	10	1	1	1	1	1
	R1-02	15	1	1	1	1	1
	R1-03	15	1	1	1	1	1
Total RFP Points		100	3	3	3	3	3
RFP Ranking			1	1	1	1	1